(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年4 月29 日 (29.04.2004)

PCT

(10) 国際公開番号
WO 2004/036840 A1

(51) 国際特許分類[7]: H04L 12/56, 9/00

(21) 国際出願番号: PCT/JP2003/013218

(22) 国際出願日: 2003 年10 月15 日 (15.10.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2002-302924
2002 年10 月17 日 (17.10.2002) JP
特願 2002-340582
2002 年11 月25 日 (25.11.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市大字門真１００６番地 Osaka (JP).

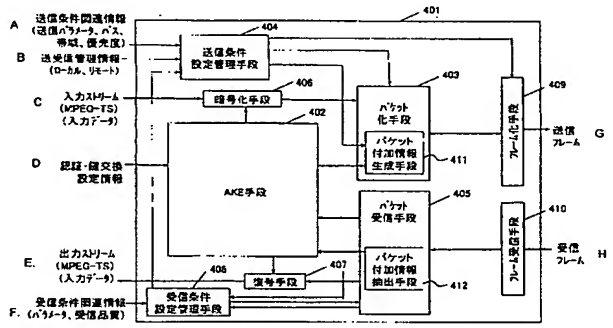
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 森岡 芳宏 (MORIOKA,Yoshihiro) [JP/JP]; 〒639-0261 奈良県香芝市 尼寺三丁目４７６−５１ Nara (JP). 綾木 靖 (AYAKI,Yasushi) [JP/JP]; 〒572-0037 大阪府 寝屋川市 葛原新町１３−１−２０６ Osaka (JP). 三谷 浩 (MITANI,Hiroshi) [JP/JP]; 〒575-0044 大阪府 四條畷市 二丁通町５−１４ Osaka (JP). 臼木 直司 (USUKI,Naoshi) [JP/JP]; 〒614-8331 京都府 八幡市 橋本意足２６−１２ Kyoto (JP).

[続葉有]

(54) Title: PACKET TRANSMISSION/RECEPTION DEVICE

(54) 発明の名称: パケット送受信装置



A ..TRANSMISSION CONDITION-RELATED INFORMATION (TRANSMISSION PARAMETER, PATH, BAND, PRIORITY)
B...TRANSMISSION/RECEPTION MANAGEMENT INFORMATION (LOCAL, REMOTE)
C...INPUT STREAM (MPEG-TS) (INPUT DATA)
D...AUTHENTICATION/KEY EXCHANGE SETTING INFORMATION
E...OUTPUT STREAM (MPEG-TS)(INPUT DATA)
F...RECEPTION CONDITION-RELATED INFORMATION (PARAMETER, RECEPTION QUALITY)
404...TRANSMISSION CONDITION SETTING MANAGEMENT MEANS
406...ENCRYPTION MEANS
402...AKE MEANS
407...DECRYPTION MEANS
408...RECEPTION CONDITION SETTING MANAGEMENT MEANS
403...PACKETIZING MEANS
411...PACKET ADDITION INFORMATION CREATION MEANS
405...PACKET RECEPTION MEANS
412...PACKET ADDITION INFORMATION EXTRACTION MEANS
409...FRAMING MEANS
410...FRAME RECEPTION MEANS
G...TRANSMISSION FRAME
H...RECEPTION FRAME

(57) Abstract: A packet transmission/reception device includes: authentication/key exchange means; encryption means for creating encrypted transmission data; transmission condition setting management means for creating transmission condition setting information for setting a transmission condition of a transmission packet; packetizing means for creating a transmission packet by using the encrypted transmission data; reception condition setting management means for creating reception condition setting information for setting a reception condition of a reception packet; packet reception means for receiving the reception packet; and decryption means for decrypting the reception data by using a decryption key.

(57) 要約: パケット送受信装置であって、認証・鍵交換手段と、暗号化送信データを生成する暗号化手段と、送信パケットの送信条件を設定する送信条件設定情報を生成する送信条件設定管理手段と、暗号化送信

[続葉有]

WO 2004/036840 A1

(74) 代理人: 山本 秀策, 外(YAMAMOTO,Shusaku et al.); 〒540-6015 大阪府 大阪市中央区 城見一丁目２番２７号クリスタルタワー１５階 Osaka (JP).

(81) 指定国 (国内): CN, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

データを用いて、送信パケットを生成するパケット化手段と、受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、受信パケットを受信するパケット受信手段と、復号鍵を用いて受信データを復号する復号手段とを備える。

明　細　書

パケット送受信装置

技術分野

本発明は、パケット送受信装置に関する。より詳細には、本発明は、暗号化されたデータ（例えば、ＡＶデータ）を用いてパケットを生成し、生成したパケットを、ＩＥＥＥ　８０２．３規格などに準拠するイーサネット（Ｒ）（有線ＬＡＮ）、または、ＩＥＥＥ　８０２．１１規格などに準拠する無線ＬＡＮなどを用いて、送信および受信するパケット送受信装置に関する。

背景技術

従来、一般家庭においても、ＩＥＥＥ　１３９４規格を用いてＩＥＣ　６１８３－４で規定された方式に基づいて、ＭＰＥＧ－ＴＳを暗号化して伝送することが行われている。ＭＰＥＧ－ＴＳなどのＡＶデータを暗号化して伝送する方式の一例としては、ＤＴＣＰ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ）方式が規定されている。

ＤＴＣＰ方式は、ＩＥＥＥ　１３９４規格、ＵＳＢなどの伝送メディア上のコンテンツ保護に関する方式である。ＤＴＣＰ方式は、ＤＴＬＡ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｌｉｃｅｎｃｉｎｇ　Ａｄｍｉｎｉｓｔｒａｔｏｒ）で規格化されている。ＤＴＣＰ方式は、より詳細には、例えば、ｈｔｔｐ：／／ｗｗｗ．ｄｔｃｐ．ｃｏｍ、ｈｔｔｐ：／／ｗｗｗ．ｄｔｃｐ．ｃｏｍ／ｄａｔａ／ｄｔｃｐ＿ｔｕｔ．ｐｄｆ、ｈｔｔｐ：／／ｗｗｗ．ｄｔｃｐ．ｃｏｍ／ｄａｔａ／ｗｐ＿ｓｐｅｃ．ｐｄｆ、および、書籍「ＩＥＥＥ１３９４、ＡＶ機器への応用」、高田信司監修、日刊工業新聞社、「第８章、コピープロテクション」、１３３～１４９ページに説明されている。

図３８は、ＤＴＣＰ方式を用いて、ＭＰＥＧ―ＴＳを、ＩＥＥＥ　１３９４規格に準拠する伝送メディアを介して伝送すること示す模式図である。

ＤＴＣＰ方式では、送信装置をソース２００１、受信装置をシンク２００２とよび、暗号化したＭＰＥＧ－ＴＳなどのデータはソース２００１からネットワーク２００３を介して、シンク２００２に伝送される。

図３８において、ソース２００１は、例えば、ＤＶＨＳ、ＤＶＤレコーダ、１３９４搭載ＳＴＢ（Ｓｅｔ　Ｔｏｐ　Ｂｏｘ）または１３９４搭載ディジタルＴＶ（Ｔｅｌｅｖｉｓｉｏｎ）であり、シンク２００２は、例えば、ＤＶＨＳ、ＤＶＤレコーダ、１３９４搭載ＳＴＢ（Ｓｅｔ　Ｔｏｐ　Ｂｏｘ）または１３９４搭載ディジタルＴＶ（Ｔｅｌｅｖｉｓｉｏｎ）である。

このように、ＤＴＣＰ方式を用いて、ＩＥＥＥ　１３９４規格に準拠する伝送メディアを介してＭＰＥＧ―ＴＳなどのＡＶデータを伝送することが知られている。

しかしながら、ＤＴＣＰ方式をインターネットの標準プロトコルであるＩＰプロトコルに実装することは、今日まで知られていない。したがって、ＤＴＣＰ方式を用いて、ＡＶデータを、イーサネット（Ｒ）の規格であるＩＥＥＥ　８０２．３規格、無線ＬＡＮの規格であるＩＥＥＥ　８０２．１１規格、または、その他のＩＰパケットを伝送可能な伝送メディアを介して伝送することはできなかった。別の言い方でいうと、従来においては、ＩＰプロトコルを介して論理的に接続された送信装置と受信装置との間を、暗号化を用いてデータの機密性および著作権の保護を行なった状態でＭＰＥＧ－ＴＳなどのＡＶデータを伝送することはできなかった。

発明の開示

本発明によれば、送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、暗号化鍵および復号鍵を生成する認証・鍵交換手段と、前記

暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも１つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定するための受信条件設定情報を生成する受信条件設定管理手段と、前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、前記復号鍵を用いて前記受信データを復号する復号手段とを備える。

前記パケット化手段は、前記送信条件設定情報および前記認証・鍵交換手段に関連する認証・鍵交換関連情報の少なくとも１つを用いて、パケット付加情報を生成するパケット付加情報生成手段を含み、前記パケット化手段は、前記暗号化送信データに前記パケット付加情報を付加することによって、前記送信パケットを生成し、前記パケット受信手段は、前記送信パケットに含まれるパケット付加情報を抽出するパケット付加情報抽出手段を含む。

前記送信パケットを用いて送信フレームを生成するフレーム化手段と、受信フレームを受け取り、前記受信フレームから前記受信パケットを抽出するフレーム受信手段とをさらに備える。

前記パケット化手段にて生成された第１のパケットを一時的に蓄積する第１のキュー手段と、前記パケット化手段にて生成された第２のパケットを一時的に蓄積する第２のキュー手段と、前記送信条件設定情報に基づいて、前記第１のキュー手段に蓄積された前記第１のパケットおよび前記第２のキュー手段に蓄積され

た前記第２のパケットのいずれを送信するかを制御する送信キュー制御手段と、前記第１のキュー手段から出力された第１のパケットおよび第２のキュー手段から出力された第２のパケットをフレーム化することによって送信フレームを生成するフレーム化手段と、受信フレームから前記受信パケットを抽出するフレーム受信手段とをさらに備える。

前記送信キュー制御手段は、前記第１のパケットまたは前記第２のパケットの送信経路に関する情報と、前記第１のパケットまたは前記第２のパケットを送信するのに必要な帯域幅に関する情報と、前記送信パケットの送信から到着までの遅延に関する情報と、前記第１のパケットまたは前記第２のパケットの優先度に関する情報とのうち少なくとも１つの情報を用いて、前記第１のキュー手段に蓄積された前記第１のパケットおよび前記第２のキュー手段に蓄積された前記第２のパケットのいずれを送信するかを制御する。

前記送信キュー制御手段は、ＩＥＴＦ　ｒｆｃ２２０５、ｒｆｃ２２０８、ｒｆｃ２２０９で記載されたＲＳＶＰ方式、ＩＥＴＦ　ｒｆｃ２２１０、ｒｆｃ２２１１、２２１２，ｒｆｃ２２１５で記載されたＩｎｔｓｅｒｖ方式、ＩＥＴＦ　ｒｆｃ２４７４、ｒｆｃ２４７５、ｒｆｃ２５９７、ｒｆｃ２５９８で記載されたＤｉｆｆｓｅｒｖ方式のいずれか１つの制御方式を使用する。

前記送信キュー制御手段は、前記第１のキュー手段に蓄積された前記第１のパケットおよび前記第２のキュー手段に蓄積された前記第２のパケットのうちのいずれかを選択して、選択したパケットを優先的に出力するように前記第１のキュー手段および前記第２のキュー手段を制御する。

前記送信キュー制御手段は、前記第２のキュー手段に蓄積された前記第１のパケットの量が所定の量を超えない場合には、前記第１のキュー手段に蓄積された前記第１のパケットを優先して出力し、前記第２のキュー手段に蓄積された前記第２のパケットの量が所定の量を超える場合には、前記第２のキュー手段に蓄積された前記第２のパケットを優先的に出力するように前記第１のキュー手段およ

び前記第２のキュー手段を制御する。

前記送信キュー制御手段は、前記第１のキュー手段から送信される前記第１のパケットと前記第２のキュー手段から送信される前記第２のパケットとの間隔を平均化するように前記第１のキュー手段および前記第２のキュー手段を制御する。

前記送信条件設定管理手段および前記受信条件設定管理手段は、前記送信フレームの送信から到着するまでの間において前記送信パケットの送信先から受信先までの経路における最大伝送パケットサイズの検出を行ない、前記最大伝送パケットサイズ情報を用いて、前記送信条件設定情報および前記受信条件設定情報を生成する。

前記フレーム化手段は、前記パケット化手段にて生成された前記送信パケットに、ＩＥＥＥ　８０２．３規格のフレームヘッダを付加する。

前記フレーム化手段は、前記パケット化手段にて生成された前記送信パケットに、ＩＥＥＥ　８０２．１Ｑ規格のフレームヘッダを付加する。

前記パケット化手段は、前記暗号化送信データを所定の大きさに変換し、ＩＥＴＦでＩＰｖ４またはＩＰｖ６として規定されているＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ヘッダを付加する。

前記パケット化手段は、ＩＰｖ４ヘッダのサービスタイプフィールド、または、サービスタイプフィールド内のＴＯＳ（Ｔｙｐｅ　ｏｆ　Ｓｅｒｖｉｃｅ）フィールドに優先パケットであることを示す情報を付加する。

前記パケット化手段は、ＩＰｖ６ヘッダのプライオリティフィールドに優先パケットであることを示す情報を付加する。

前記パケット化手段は、第１のパケット化手段と、第２のパケット化手段とを含み、前記第１のパケット化手段は、前記送信条件設定情報および前記認証・鍵交換関連情報の少なくとも一つの情報を用いて前記第１のパケットを生成し、前記第２のパケット化手段は、前記送信条件設定情報と、前記認証・鍵交換関連情報と、前記暗号化送信データとの少なくとも一つの情報を用いて前記第２のパケ

ットを生成する。

前記パケット化手段は、前記暗号化送信データを所定の大きさに変換し、ＩＥＴＦでＩＰｖ４またはＩＰｖ６として規定されているＩＰヘッダを付加し、前記第１のパケット化手段はソフトウエアによって構成され、前記第２のパケット化手段はハードウエアによって構成される。

前記送信データを優先データと一般データとに分離するデータ分離手段をさらに備え、前記暗号化手段は、前記優先データを暗号化し、前記第１のパケット化手段は、前記一般データを用いて第１のパケットを生成する。

前記第１のパケット化手段は、ＩＥＴＦ文書で規定されているデータ処理プロトコルであるＲＴＣＰ，ＲＴＳＰ，ＨＴＴＰ、ＴＣＰ、ＵＤＰ、ＩＰのうちの少なくとも１つのヘッダを付加する。

前記第２のパケット化手段は、データにシーケンス番号を付加するか、または、ＩＥＴＦ文書で規定されているデータ処理プロトコルであるＲＴＰ，ＵＤＰ、ＨＴＴＰ、ＴＣＰ、ＩＰのうちの少なくとも１つのヘッダを付加する。

前記優先データは、ＳＭＰＴＥ　２５９M規格で規定された非圧縮ＳＤ方式信号、または、ＳＭＰＴＥ　２９２M規格で規定された非圧縮ＨＤ形式、または、ＩＥＣ　６１８８３規格で規定されたＩＥＥＥ１３９４によるＤＶまたはＭＰＥＧ－ＴＳの伝送ストリーム形式、または、ＤＶＢ規格Ａ０１０で規定されたＤＶＢ－ＡＳＩによるＭＰＥＧ－ＴＳ形式、ＭＰＥＧ－ＰＳ形式、ＭＰＥＧ－ＥＳ形式、ＭＰＥＧ－ＰＥＳ形式の内の少なくとも一つのデータストリーム形式である。

前記第２のパケット化手段は、エラー訂正符号付加手段を含む。

前記エラー訂正符号付加手段で用いられるエラー訂正符号の方式は、リードソロモン方式、あるいはパリティ方式である。

前記暗号化鍵を示す情報は、前記フレーム化手段において前記暗号化鍵で暗号化された送信パケットを出力するより前に、前記暗号化鍵の復号情報を前記フレーム化手段から出力する。

前記暗号化鍵を示す情報は、前記暗号化鍵を用いて生成された前記暗号化送信データを含む送信パケットが送信されるときよりも、前記送信フレームの送信から前記送信フレームに対応する受信フレームの受信までの時間より前に送信される。

前記認証・鍵交換手段は、前記パケット送受信装置の位置情報と、前記送信パケットの到着先の位置情報または前記受信パケットの送信元の位置情報とが、あらかじめ決められた条件に合致する時に、認証を許可する。

前記送受信管理情報は、前記パケット送受信装置の位置情報と、前記送信パケットの到着先の位置情報または前記受信パケットの送信元の位置情報との少なくとも一方を含んでいる。

前記位置情報は、例えば、地域コード、住所、郵便番号、または、経度・緯度により範囲が指定された情報である。

前記認証・鍵交換手段は、前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元との間で、前記パケット送受信装置から前記送信パケットの到着先または前記受信パケットの受信元までの片道または往復の伝播時間があらかじめ決められた制限時間より短い時間である場合に、認証を許可する。

前記認証・鍵交換手段は、前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元との間の送受信区間において無線伝送区間が存在する場合、前記無線伝送区間ではデータをスクランブルして伝送するモードであることを確認した場合に、認証を許可する。

前記認証・鍵交換手段は、前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元との間で認証を行った場合に、前記送信パケットの到着先または前記受信パケットの送信元に関する情報を一時的に記憶する記憶手段と、前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元とが前記あらかじめ決められた条件に合致しないために

前記認証が成立しない場合に、前記記憶手段にて記憶された情報と、前記送信パケットの前記到着先に関する情報または前記受信パケットの前記送信先に関する情報とを照合し、前記パケット送受信装置と前記送信パケットの到着先または前記受信パケットの送信元との間で認証を行う、照合手段とを含む。

前記送信パケットの前記到着先に関する情報または前記受信パケットの前記送信先に関する情報は、証明書、ＭＡＣアドレスおよび生体情報の少なくとも１つを含む。

前記認証・鍵交換手段は、予め規定された認証および鍵交換を行い、所定の期間で暗号化鍵または復号鍵を更新する。

前記認証・鍵交換手段が前記復号鍵を更新するタイミングを示すタイミング情報が、前記送信パケットに付加される。

前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットのＴＣＰポート番号、またはＵＤＰポート番号を変化させることによって通知される。

前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＨＴＴＰを使用している場合、ＨＴＴＰリクエスト毎に更新される。

また、前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＨＴＴＰを使用している場合、一定のデータ量毎に変化される。

または、前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＲＴＰを使用している場合、予め決められた期間内に更新される。

前記認証・鍵交換手段におけるＤＴＣＰ方式のコピー制御情報は、前記送信パケットに暗号化モード情報を付加することによって伝送される。

前記優先データのデータレートが所定の値より小さくならないように、前記送信キュー制御手段は前記第１のキュー手段および前記第２のキュー手段を制御する。

前記送信キュー制御手段は、前記優先データが前記第２のキュー手段に蓄積さ

れる時間があらかじめ決めた値より常に小さくなるように、前記送信キュー制御手段は前記第１のキュー手段および前記第２のキュー手段を制御する。

前記第２のパケット化手段は、データを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、前記第２のパケットのパケットヘッダを生成するパケットヘッダ生成手段と、前記パケットヘッダと前記バッファから出力されるペイロードとを組み合わせてパケットを合成するパケット合成手段とを含み、前記パケットヘッダ生成手段は前記第２のパケットのペイロード長を指定して、前記バッファ手段に蓄積されたデータを読み出して、前記パケット合成手段に入力する。

前記第２のパケット化手段は、前記優先データから抽出したデータを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、パケット化情報を用いてパケットヘッダを生成するパケットヘッダ生成手段と、前記パケットヘッダとペイロードとを組み合わせてパケットを生成するパケット生成手段とを含み、前記カウンタ手段は前記バッファ手段からペイロード長に相当するデータを読み出すための制御データを出力する。

前記第２のパケット化手段は、データを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、パケット化情報を用いてパケットヘッダを生成するパケットヘッダ生成手段と、前記データにエラー訂正を付加するエラー訂正付加手段手段と、前記パケットヘッダと前記エラー訂正を付加したデータとを合成するパケット合成手段とを含み、前記カウンタ手段は前記バッファ手段よりペイロード長に相当するデータを読み出すための制御データを出力する。

前記優先データおよび前記一般データが処理されるレイヤよりも下位レイヤの受信フレームを処理するレイヤにおいて、前記受信フレームに含まれる受信パケットの通信プロトコルヘッダから前記優先データと前記一般データを選別して、前記優先データの処理と前記一般データの処理を独立に行う。

前記第２のパケット化手段は、暗号鍵切替手段を含み、前記暗号鍵切替手段に入力される暗号鍵を指定されたタイミングで切り替えながら前記暗号化手段に入力し、前記暗号化手段における暗号化鍵を指定の間隔で切替る。

前記暗号鍵切替に用いるタイミングとしては、前記パケットヘッダ生成手段の出力であるパケットヘッダ内の所定のシーケンス番号に同期して発生したタイミングである。

前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＨＴＴＰを使用している場合、ＨＴＴＰリクエスト毎に更新される。

また、前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＨＴＴＰを使用している場合、一定のデータ量毎に変化される。

または、前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＲＴＰを使用している場合、予め決められた期間内に更新される。

前記暗号鍵切替に用いるタイミングとしては、エラー訂正マトリックスの終点または始点に同期して発生したタイミングである。

本発明によれば、上記課題を解決するために、ネットワークを介して論理的に接続されたパケット送受信装置は、ＭＰＥＧ－ＴＳなどの送信データの機密性および著作権の保護を実現するための認証・鍵交換手段（ＡＫＥ手段）と、送信データを暗号化する暗号化手段と、送信データを用いて送信パケットを生成するパケット化手段と、暗号化された送信データを復号する復号手段と、送信パケットの送信先からフィードバックされるパケット受信状況に基づいて適切なパケット送信条件を設定する送信条件設定管理手段と、パケット受信手段と、受信条件設定管理手段とを備える。

これにより、ＤＴＣＰ方式をインターネットの標準プロトコルであるＩＰプロトコルに実装することができる。

また、ＭＰＥＧ－ＴＳなどのＡＶデータを送信装置で暗号化してデータの機密性および著作権の保護などを図り、パケット（例えば、ＩＰパケット）を伝送可

能なネットワークを介して伝送し、受信装置で暗号化されたデータを復号することが可能である。

本発明のある実施の形態によれば、パケット化手段において、送信パケットを一般パケットと、リアルタイム性が高く、優先的に送信されるべき優先パケットとにクラス分けし、一般パケットを第１のデータキュー手段に、また、優先パケットを第２のデータキュー手段に入力する。そして、送信キュー制御手段は、第１のデータキュー手段および第２のデータキュー手段に一時的に蓄積されているパケットの送信順序を制御する。これにより、データの機密性および著作権の保護を図りながら、リアルタイム性の高いデータを優先的に伝送することができる。

また、入力ストリームが２チャネル以上の複数ストリームである場合、各々のストリームに関係する信号を優先データと一般データにクラス分けしてもよい。

本発明のある実施の形態によれば、パケット化手段は、第１のパケット化手段と第２のパケット化手段とを含んでいる。第１のパケット化手段には、ＡＫＥ関連情報を含む一般データが入力される。第２のパケット化手段には、暗号化手段にて生成された暗号化送信データおよびＡＫＥ関連情報が入力される。第２のパケット化手段では、ハードウエアによってパケットが生成される。なお、ＡＫＥ関連情報とは、コピー制御情報または暗号化鍵更新情報のことである。

第１のパケット化手段にて生成されたパケットは、第１のデータキュー手段に入力されて一時的に蓄積され、第２のパケット化手段にて生成されたパケットは第２のデータキュー手段に入力されて、一時的に蓄積される。

送信条件設定管理手段が、送信キュー制御手段に、第２のデータキュー手段に一時的に蓄積されているパケットを優先的に出力するように命令すると、暗号化されたデータが優先的に出力される。この制御において、第２のデータキュー手段がオーバフローしないように制御し、受信装置が適切な大きさのバッファを有する場合、送信装置と受信装置との間でコンテンツのリアルタイム伝送が実現できる。

以上、送信装置と受機装置との間でデータを暗号化してリアルタイム伝送する場合に、第２のパケット化手段はハードウエアで構成されているため、ソフトウエア処理が間に合わないために発生する送信パケットの送り残しおよび受信パケットの取りこぼしといった不具合が発生しない。また、データ量の小さい第１のパケット化手段は安価なマイコンなどでも構成できるため、低コスト化を図ることができる。

本発明のある実施の形態によれば、機器認証と暗号化鍵の交換を行なうＡＫＥ手段は、ＤＴＣＰ方式に基づいた方式であり、暗号化鍵生成手段と、ＤＴＣＰ情報生成手段と、ＡＫＥコマンド送信処理手段と、ＡＫＥコマンド受信処理手段と、交換鍵生成手段と、暗号化鍵変更情報生成手段と、復号鍵生成手段とを備える。暗号化鍵生成手段は、暗号化鍵を生成し暗号化に入力し暗号化動作を設定する。ＤＴＣＰ情報生成手段は、外部から入力されるコピー制御情報、および、暗号化鍵生成手段から入力される鍵更新情報とを用いて、ＡＫＥ関連情報を生成する。ＡＫＥコマンド送信処理手段は、暗号化鍵生成手段より暗号化鍵を、外部よりＡＫＥパラメータを、さらにＡＫＥコマンド受信処理手段よりＡＫＥコマンド情報を受け取り、ＡＫＥ送信コマンドを生成し出力する。ＡＫＥコマンド受信処理手段は、第１のパケット受信手段よりＡＫＥ設定制御情報を受け取り、ＡＫＥ送信処理手段、交換鍵生成手段、暗号化鍵変更情報生成手段にそれぞれ設定制御情報を出力する。暗号化鍵変更情報生成手段は、ＡＫＥコマンド受信処理手段と第１のパケット受信手段より情報を得て暗号化鍵変更情報を生成する。復号鍵生成手段は、交換鍵生成手段と暗号化鍵変更情報生成手段からの情報を用いて、復号鍵を生成し復号手段に出力する。

本発明のある実施の形態によれば、暗号化手段にて生成された暗号化送信データ、および、コピー制御情報および暗号化鍵更新情報などのＡＫＥ関連情報が入力される第２のパケット化手段が、内部にエラー訂正符号付加手段を備え、これらの情報にエラー訂正符号を付加し、ＵＤＰ／ＩＰプロトコルにより伝送される。

これにより、ＩＰパケットの伝送において、ネットワークでパケットロスおよびビットエラーなどが発生した場合にも、受信装置でエラー訂正により送信データの復元が可能となる。

本発明のある実施の形態によれば、優先して送信される優先パケットと、この優先パケットよりも送信優先度が低い一般パケットとを時間軸上で多重して送信し、送信される優先パケットにおける優先データの平均送信データレートを、たとえば、専用ハードウエアを用いて平均入力レート以上の速度で送信するように制御する。

また、一般データは一時的にバッファ手段に蓄積され、優先データ伝送が優先して行なわれる中で間欠的に伝送される。ここで、一般データの伝送レートが１Ｍｂｐｓ以下の場合は、安価なＣＰＵまたはマイコンなどのプロセッサを用いて一般伝送の伝送処理が可能である。

なお、ストリームとして入力される優先データでは、ストリームの無効データ部が除去され、有効データのみを用いて、パケット化情報に基づいてパケットが生成される。ここで、通信プロトコルとしてＵＤＰ／ＩＰを使用すると、ヘッダとしては、アドレスとしてＩＰアドレス、また、サブアドレスとしてＵＤＰポート番号を使用することとなる。

本発明のある実施の形態によれば、有効データから優先データフォーマット情報を得て、外部から入力されるパケット化情報と共にパケット化パラメータの決定に使用する。これにより、たとえば、優先データがＤＶ系の場合はＤＩＦブロックの８０バイト単位、また、ＭＰＥＧ系の場合はＴＳパケットの１８８バイト単位で優先データのパケット化の自動化などを行なうことができ、送受信装置の構成を簡単にすることができる。

本発明のある実施の形態によれば、送信装置内の優先データパケット化手段において、優先データにエラー訂正符号を付加することにより、ネットワークにおいてパケットロスが発生した場合にも、受信装置で優先データを復元することが

できる。

本発明のある実施の形態は、送信装置内の優先データパケット化手段における伝送エラー保護機能に関し、優先データを暗号化した後、エラー訂正符号を付加することにより、ネットワークにおいてパケットロスが発生した場合にも、受信装置で優先データを復元することが可能になるとともに、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現する。これにより、伝送路にインターネットなど公衆網を使用した場合においても、リアルタイム伝送される優先データ（ＡＶデータ）の盗聴、漏洩を防止することができる。また、インターネット等で伝送されるＡＶデータの販売、課金が可能となり、安全性の高いＢ－Ｂ、Ｂ－Ｃのコンテンツ販売流通が可能となる。

本発明のある実施の形態は、暗号化を行なう暗号鍵を切り替える方法に関し、エラー訂正マトリックスの位相を暗号鍵の切替位相とすることにより、暗号鍵の切替をスムーズに実行することが可能となる。

本発明のある実施の形態は、有効データパケットのパケットヘッダのポート番号設定に関し、優先データのフォーマットまたはチャネル番号とポート番号の組み合わせを決めるテーブルを送信装置および受信装置で設けることにより、受信装置でポート番号を検出するだけでフォーマット検出ができるため、受信装置での信号処理を簡単にすることが可能となる。

また、２系統のストリーム処理が可能な受信装置で２つのストリームを同時受信している場合でもポート番号でフォーマットまたはチャネルの識別が可能となる。

図面の簡単な説明

図１は、本発明を適用可能なシステムの一例を示す図である。

図２は、認証および鍵交換にＤＴＣＰ方式を適用する場合の送信装置および受信装置の動作を示すための図である。

図３は、ＤＴＣＰ方式をイーサネット（Ｒ）を用いて、２階建ての家屋に適用した場合の一例を示す模式図である。

図４は、本発明の実施の形態１によるパケット送受信装置のブロック図である。

図５は、ＭＰＥＧ－ＴＳを用いて、パケットさらには、フレームを生成して、伝送する場合のパケット形式の一例を示す模式図である。

図６は、本発明の実施の形態１によるプロトコルスタックを説明するための模式図である。

図７は、本発明の実施の形態２によるパケット送受信装置のブロック図である。

図８は、本発明の実施の形態３によるパケット送受信装置のブロック図である。

図９は、本発明の実施の形態３によるプロトコルスタックによる説明図である。

図１０は、ＭＰＥＧ－ＴＳを用いて、パケットさらには、フレームを生成して、伝送する場合のパケット形式の一例を示す模式図である。

図１１は、本発明の実施の形態４のパケット送受信装置のブロック図である。

図１２は、本発明の実施の形態４におけるパケット化手段およびパケット受信手段を説明するためのブロック図である。

図１３は、本発明の実施の形態５におけるパケット化手段およびパケット受信手段を説明するためのブロック図である。

図１４は、本発明の実施の形態５のプロトコルスタックの模式図である。

図１５は、エラー訂正方式がリードソロモン方式である場合の模式図である。

図１６は、エラー訂正方式がパリティ方式である場合の模式図である。

図１７は、本発明の実施の形態６によるパケット送受信装置のブロック図である。

図１８は、本発明の実施の形態６の別の形態によるパケット送受信装置のブロック図である。

図１９は、本発明の実施の形態７によるパケット送信手段のブロック図である。

図２０は、優先パケットのプロトコルスタックの模式図である。

図２１は、優先パケットと一般パケットの伝送タイミングの模式図である。

図２２は、本発明の実施の形態７の変形例によるパケット送信手段のブロック図である。

図２３は、本発明の実施の形態８によるパケット送信手段のブロック図である。

図２４は、本発明の実施の形態８の変形例によるパケット送信手段のブロック図である。

図２５は、本発明の実施の形態９によるパケット送信手段のブロック図である。

図２６は、本発明の実施の形態９の変形例による優先データパケット化手段のブロック図である。

図２７は、本発明の実施の形態９の別の変形例による優先データパケット化手段のブロック図である。

図２８は、エラー訂正がパリティ処理方式の場合のパケット構成を示す図である。

図２９は、エラー訂正がリードソロモン方式の場合のパケット構成を示す図である。

図３０は、本発明の実施の形態１０のパケット送信手段のブロック図である。

図３１は、本発明の実施の形態１０の優先データパケット化手段のブロック図である。

図３２は、本発明の実施の形態１１の優先データパケット手段のブロック図である。

図３３は、暗号の切り替えタイミングを説明するための模式図である。

図３４は、本発明の実施の形態１２による優先データパケット手段のブロック図である。

図３５は、本発明の実施の形態１３によるＩＥＥＥ１３９４ストリーム伝送に適用したパケット送信システムのブロック図である。

図３６は、本発明の実施の形態１３によるＳＤＩ／ＳＤＴＩ／ＤＶＢ－ＡＳＩ

ストリームの伝送に適用したパケット送信システムのブロック図である。

図３７は、本発明の実施の形態１３のパケット送受信装置のブロック図である。

図３８は、ＤＴＣＰ方式を用いて、ＭＰＥＧ－ＴＳを、ＩＥＥＥ　１３９４規格に準拠する伝送メディアを介して伝送することを示す模式図である。

発明を実施するための最良の形態

本願明細書の以下の説明において、パケットを含む情報を送信および受信可能な装置を送受信装置とよぶ。２つの送受信装置はお互いに情報を通信する。また、本願明細書の以下の説明では、便宜上、送信すべきデータ（例えば、ＡＶデータ）を送信する送受信装置を「送信装置」とよび、送信装置によって送信されたそのようなデータを受信する送受信装置を「受信装置」とよぶ。

まず、始めに、本発明を明確にするために本発明を適用可能なシステムの概略について説明する。

図１は、本発明を適用可能なシステムの一例を示す図である。

送信装置１０１は、データをルータ１０２を介して、受信装置１０３に送信する。

より詳細には、送信装置１０１には、送受信条件関連情報、認証・鍵交換（Ａｕｔｈｅｎｔｉｆｉｃａｔｉｏｎ　ａｎｄ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ、以下、ＡＫＥともよぶ）設定情報、入力ストリーム（ＭＰＥＧ－ＴＳなどのデータ）が入力され、以下の手順１から手順３に基づいて、通信が実行される。

手順１）送受信パラメータの設定：

（１－１）送信装置１０１および受信装置１０３のＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレス、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレス、ＴＣＰ／ＵＤＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ／Ｕｓｅｒ　Ｄａｔａｇｒａｍ　Ｐｒｏｔｏｃｏｌ）ポート番号等を設定する。

（１－２）送信信号の種別、帯域を設定する。

送信装置１０１および受信装置１０３は、ＱｏＳ（Ｑｕａｌｉｔｙ ｏｆ Ｓｅｒｖｉｃｅ）エージェントとして機能し、ルータ１０２は、ＱｏＳマネージャとして機能する。ＱｏＳエージェントとＱｏＳマネージャとの間でＩＥＥＥ ８０２．１Ｑ（ＶＬＡＮ）規格を用いたネットワークに関する設定が行われる。

（１－３）ＩＥＥＥ ８０２．１Ｑ／ｐ規格に基づいて優先度が設定される。

手順２）認証および鍵交換：

（２－１）送信装置１０１および送信装置１０３は、お互いを認証し、お互いに鍵を交換する。この場合、例えば、ＤＴＣＰ方式を用いることもできる。

手順３）データ伝送：

（３－１）送信装置１０１から受信装置１０３に暗号化されたデータ（例えば、ＭＰＥＧ－ＴＳ）が伝送される。

なお、図１では、入力ストリームとして、ＭＰＥＧ－ＴＳが送信装置１０１に入力されているが、本発明は、これに限定されない。このような入力ストリームとしては、例えば、ＭＰＥＧ１／２／４などのＭＰＥＧ－ＴＳストリーム（ＩＳＯ／ＩＥＣ １３８１８）、ＤＶ（ＩＥＣ ６１８３４、ＩＥＣ ６１８８３）、ＳＭＰＴＥ ３１４Ｍ（ＤＶ－ｂａｓｅｄ）、ＳＭＰＴＥ ２５９Ｍ（ＳＤＩ）、ＳＭＰＴＥ ３０５Ｍ（ＳＤＴＩ）、ＳＭＰＴＥ ２９２Ｍ（ＨＤ－ＳＤＩ）等で規格化されたストリームがある。

なお、送信装置１０１から送信されるデータとしては、一般的なＡＶデータであってもよい。さらに、本発明のデータは、ファイルであってもよい。データとしてファイルを転送する場合、送信装置１０１と受信装置１０３との間の伝播遅延時間と、送信装置１０１と受信装置１０３のそれぞれの処理能力との関係から、データ転送速度がＡＶデータの通常再生データレートよりも大きくなるなどの条件下において、リアルタイムよりも高速にデータを伝送することが可能になる。

次に、図２を参照して、上記手順２の認証および鍵交換に関して、さらに詳細

に説明する。

図２は、認証および鍵交換にＤＴＣＰ方式を適用する場合の送信装置および受信装置の動作を示すための図である。

ここでは、ＤＴＣＰ方式に準拠した認証と鍵交換（Ａｕｔｈｅｎｔｉｆｉｃａｔｉｏｎ　ａｎｄ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ、以下、ＡＫＥともよぶ）が行なわれている。その場合、送信装置１０１をＡＫＥソースともよび、受信装置１０３をＡＫＥシンクともよぶ。

送信装置１０１と受信装置１０３との間はＩＰネットワークにより接続されている。

まず、送信装置１０１から受信装置１０３にデータのコピー保護情報を含んだデータの保護モード情報が送信される。ここで、送信装置１０１は、暗号化データを同時に送信してもよい。

受信装置１０３は、データのコピー保護情報を解析し、使用する認証方式を決定して認証要求を送信装置１０１に送る。これらの動作を行うことによって、送信装置１０１および受信装置１０３は認証鍵を共有する。

次に、送信装置１０１は認証鍵を用いて交換鍵を暗号化することによって、暗号化交換鍵を生成し、送信装置１０１は、暗号化交換鍵を受信装置１０３に送信する。受信装置１０３は、送信装置１０１と共有している認証鍵を用いて、暗号化交換鍵を復号して、交換鍵を生成する。

次いで、送信装置１０１は暗号化鍵を時間的に変化させるために、時間とともに変更する鍵変更情報を生成する。ここで、この鍵変更情報は、シード情報ともよばれる。送信装置１０１は、鍵変更情報を受信装置１０３に送信する。

送信装置１０１は、交換鍵と鍵変更情報とを用いて暗号化鍵を生成して、データ（例えば、ＭＰＥＧ－ＴＳ）をこの暗号化鍵を用いて暗号化手段で暗号化することによって、暗号化データを生成し、この暗号化データを受信装置１０３に送信する。

受信装置１０３は、鍵変更情報と交換鍵とを用いて、暗号化鍵を生成する。受信装置１０３ではこの暗号化鍵を用いて暗号化データを復号する。受信装置１０３において暗号化鍵を復号鍵ともよぶ。

なお、送信装置１０１および受信装置１０３は、その後、任意の時間に、お互いの鍵変更情報を確認してもよい。

図３は、ＤＴＣＰ方式をイーサネット（Ｒ）を用いて、２階建ての家屋に適用する場合の一例を示す模式図である。

１階のネットワーク構成３０１は、ルータ３０３を含んでおり、ルータ３０３は、１階に設置されている。１階のネットワーク構成３０１、１００Ｍｂｐｓの ＦＴＴＨ（Ｆｉｂｅｒ　ｔｏ　ｔｈｅ　Ｈｏｍｅ）を介してインターネットに接続されている。

２階のネットワーク構成３０２は、スイッチングハブ３０４を含んでおり、スイッチングハブ３０４は、２階に設置されている。

ルータ３０３は、ネットワーク３０５を介して、スイッチングハブ３０４に接続されており、それにより、１階のネットワーク構成３０１は、２階のネットワーク構成３０２に接続されている。ここで、ネットワーク３０５は、ルータ３０３とスイッチングハブ３０４とを接続するイーサネット（Ｒ）ネットワークであり、ルータ３０３は、スイッチングハブとしても機能している。

家屋の全てのイーサネット（Ｒ）ネットワークのデータレートは１００Ｍｂｐｓである。

１階のネットワーク構成３０１では、ルータ３０３には、テレビ（ＴＶ（Ｔｅｌｅｖｉｓｉｏｎ））、パソコン（ＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ））およびＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）レコーダが１００Ｍｂｐｓのイーサネット（Ｒ）で接続され、また、エアコンおよび冷蔵庫がＥＣＨＯＮＥＴで接続されている。

また、２階のネットワーク構成３０２では、スイッチングハブ３０４には、テ

レビ（ＴＶ）、パソコン（ＰＣ）およびＤＶＤレコーダが１００Ｍｂｐｓのイーサネット（Ｒ）で接続され、また、エアコンがＥＣＨＯＮＥＴで接続されている。ＥＣＨＯＮＥＴは「エコーネットコンソーシアム」（ｈｔｔｐ：／／ｗｗｗ．ｅｃｈｏｎｅｔ．ｇｒ．ｊｐ／）で開発された伝送方式である。

図３において、パソコン（ＰＣ）、ＤＶＤレコーダ、ルータ３０３およびスイッチングハブ３０４は、ＩＥＥＥ　８０２．１Ｑ規格（ＶＬＡＮ）に対応している。したがって、各ポートのデータレートが全て同じ（例えば１００Ｍｂｐｓ）である。ルータ３０３およびスイッチングハブ３０４において、特定の出力ポートから出力されるデータレートの合計がそのポートの出力ポートの伝送レートの規格値または実効値を越えないかぎり、入力ポートから入力されたデータは、ルータ３０３またはスイッチングハブ３０４内部で失われることなく、全て出力ポートから出力される。

スイッチングハブ３０４に、たとえば８個の入力ポートを介してデータが同時に入力されても、それぞれのデータの出力ポートが異なっていれば、それぞれのデータは、ルータ３０３またはスイッチングハブ３０４の内部に設けられたバッファにおいて競合することなく、スイッチングされて出力ポートから出力される。したがって、入力ポートから入力されたデータはパケット落ちすることなく全て出力ポートから出力される。

図３では、家屋内の全てのイーサネット（Ｒ）のデータレートが１００Ｍｂｐｓであり、１階と２階との間のネットワーク３０５のデータレートも１００Ｍｂｐｓである。１階の機器と２階の機器との間で複数のデータが流れる場合、各データに対するデータレートの制限がないと、このネットワーク３０５上を流れるデータレートの合計が１００Ｍｂｐｓを越える可能性があり、ＭＰＥＧ－ＴＳの映像アプリケーションなどのリアルタイムな伝送が必要とされるデータストリームが途切れる可能性がある。

この場合、リアルタイムな伝送が必要とされるデータストリームが途切れない

ようにするには、伝送データに対して優先制御を行うことが必要である。端末だけでなく、ルータ３０３およびスイッチングハブ３０４に、後述するストリーム伝送およびファイル転送の速度制限機構などを導入することによって、リアルタイムな伝送が必要とされるデータストリームを途切れないようにすることができる。

例えば、リアルタイムな伝送が必要とされるＭＰＥＧ－ＴＳデータの伝送優先度をファイルデータの伝送優先度よりも高くすると、１階のＰＣと２階のＰＣとの間でファイル転送を行いながら、同時に、１階のＤＶＤレコーダ、ＰＣまたはＴＶと、２階のＤＶＤレコーダ、ＰＣまたはＴＶとの間でＭＰＥＧ－ＴＳデータを暗号化してリアルタイムで伝送することが可能となる。

ルータ３０３またはスイッチングハブ３０４における伝送速度制限機構は、データ流入制御により実現できる。より具体的には、ルータ３０３またはスイッチングハブ３０４の入力データキュー手段において優先度の高いデータと低いデータとを比較して、優先度の高いデータを優先的に出力することにより実現できる。この優先制御方式に用いるバッファ制御ルールとしては、ラウンドロビン方式、流体フェアスケジューリング方式、重み付けフェアスケジューリング方式、自己同期フェアスケジューリング方式、ＷＦＦＱ方式、仮想時計スケジューリング方式、クラス別スケジューリング方式などがある。これらのスケジューリング方式に関する詳細は、戸田巌著、「ネットワークＱｏＳ技術」、平成１３年５月２５日（第１版）、オーム社刊の第１２章などに記述されている。

（実施の形態１）

図４は、本発明の実施の形態１によるパケット送受信装置４０１のブロック図である。

パケット送受信装置４０１は、ＤＴＣＰ方式に準拠した認証および鍵交換を行い、パケットを送信および受信する。ここで、パケット送受信装置４０１は、パ

ケット送受信装置４０１と同様の機能を有する別のパケット送受信装置にパケットを送信し、そのようなパケット送受信装置からのパケットを受信することを想定している。したがって、パケット送受信装置４０１は、送信パケットの到着先に送信パケットを送信し、受信パケットの送信元から受信パケットを受信する。

パケット送受信装置４０１は、暗号化鍵および復号鍵を生成する認証・鍵交換手段（以下、ＡＫＥ手段ともよぶ）４０２と、暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段４０６と、送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも１つを用いて、送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段４０４と、暗号化送信データを用いて、送信パケットを生成するパケット化手段４０３と、受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、受信パケットの受信条件を設定するための受信条件設定情報を生成する受信条件設定管理手段４０８と、受信パケットを受信するパケット受信手段４０５であって、受信条件設定情報を用いて、受信パケットから、受信パケットに含まれる受信データを抽出するとともに、受信パケットからパケット受信情報を生成し、パケット受信情報を認証・鍵交換手段４０２または受信条件設定管理手段４０８に出力する、パケット受信手段４０５と、復号鍵を用いて受信データを復号する復号手段４０７とを備える。

パケット送受信装置４０１は、送信パケットを用いて送信フレームを生成するフレーム化手段４０９と、受信フレームを受信するフレーム受信手段４１０とをさらに備えており、それにより、パケット送受信装置４０１は、送信パケットを含む送信フレームを送信する送信装置として機能するとともに、受信パケットを含む受信フレームを受信する受信装置としても機能する。

以下に、パケット送受信装置４０１が、ＴＣＰ／ＩＰまたはＵＤＰ／ＩＰなどを用いて送信フレームを送信する場合について説明する。

送信条件設定管理手段４０４には、送信条件関連情報と、送受信管理情報と、

受信条件設定情報とが入力される。

送信条件関連情報は、例えば、送信データの種別と、送信先アドレスまたはポート番号の情報と、送信に用いるパス情報（ルーティング情報）と、送信データの帯域と、送信データの送信優先度とを含む。

送受信管理情報は、送信装置（ローカル）および受信装置（リモート）における機器管理制御データを含む。

より詳細には、送信管理情報は、送信装置（ローカル）および受信装置（リモート）におけるＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスまたは位置情報などの機器管理制御データを含む。位置情報は、例えば、地域コード、住所、郵便番号、あるいは、経度・緯度などに範囲が指定された情報である。位置情報を用いて、認証を行う送信機器と受信機器との範囲を限定することが可能となる。また、送信装置と受信装置との間で送受信されるパケットの片道または往復の伝播時間があらかじめ決められた制限時間より短い時間である場合に、認証を許可することにより認証範囲を制限することも可能である。たとえば、Ｅｔｈｅｒｎｅｔ方式のＩＰ接続で、ＲＴＴ（Ｒｏｕｎｄ　Ｔｒｉｐ　Ｔｉｍｅ）が１ｍｓｅｃ以下である場合にのみ認証を許可することにより認証の範囲を制限することができる。また、８０２．１１ａ規格または８０２．１１ｂ規格などの無線方式とＥｔｈｅｒｎｅｔ規格などの複数の伝送メディアを組み合わせた場合には、それぞれの伝送メディアの伝播遅延特性に応じたＲＴＴを設定して認証を許可することができる。これらの時間の測定は、たとえば、ＡＫＥの専用コマンドで行ってもよいし、図５を参照して以下に説明するように、パケット付加情報がタイムスタンプまたは位置情報を含むことによって実現することもできる。

さらに、送信装置と受信装置との間の送受信区間において無線伝送区間が存在する場合、その無線伝送区間ではデータを無線ＬＡＮのセキュリティ方式であるＷＥＰまたはＷＰＡ方式によって、データの暗号化およびスクランブル化を行い伝送するモードであることを確認した後に、認証を許可することにより、無線伝

送区間でのデータ漏洩による第３者によるデータ解読を防止することができる。

受信条件設定情報は、受信装置の受信状況を受信装置から送信装置にフィードバックする情報を含む。この情報は、受信条件設定管理手段４０８から送信条件設定管理手段４０４に入力される。

送信条件設定管理手段４０４は、送信条件関連情報と、送受信管理情報と、受信条件関連情報との少なくとも１つを用いて、送信条件設定情報を生成する。送信条件関連情報は、パケット送受信装置の位置情報と、送信パケットの到着先の位置情報または受信パケットの送信元の位置情報との少なくとも一方を含んでいる。

送信条件設定管理手段４０４にて生成された送信条件設定情報を用いて、パケット化手段４０３およびフレーム化手段４０９では、ヘッダおよびペイロードなどが設定される。送信条件設定管理手段４０４は、また、送信条件設定情報をパケット化手段４０３、および、パケット化手段４０３に含まれるパケット付加情報生成手段４１１に出力する。

ＡＫＥ手段４０２には、認証・鍵交換設定情報（以下、ＡＫＥ設定情報ともよぶ）が入力される。ＡＫＥ手段４０２から、このＡＫＥ設定情報に関連した認証・鍵交換関連情報（以下、ＡＫＥ関連情報ともよぶ）がパケット付加情報生成手段４１１に入力される。認証・鍵交換関連情報は、例えば、伝送時における暗号化送信データの暗号化状態を表すコピー保護情報と、暗号化鍵変更情報とを含む。

暗号化手段４０６には、例えば、ＭＰＥＧ－ＴＳが、入力ストリームとして入力される。暗号化手段４０６は、ＭＰＥＧ－ＴＳの一部を送信データとし、ＡＫＥ手段４０２にて生成された暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する。暗号化送信データは、暗号化手段４０６からパケット化手段４０３に出力される。

パケット化手段４０３は送信条件設定管理手段４０４において生成された送信

条件設定情報に基づいて、暗号化送信データを用いて、送信パケットを生成する。

パケット化手段４０３は、パケット付加情報生成手段４１１を含み、パケット付加情報生成手段４１１は、送信条件設定情報および認証・鍵交換関連情報の少なくとも１つを用いてパケット付加情報を生成する。

パケット化手段４０３は、暗号化送信データを所定の大きさに変換し、ＩＥＴＦでＩＰｖ４またはＩＰｖ６として規定されているＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）ヘッダを付加してもよく、ＩＰｖ４ヘッダのサービスタイプフィールド、または、サービスタイプフィールド内のＴＯＳ（Ｔｙｐｅ ｏｆ Ｓｅｒｖｉｃｅ）フィールドに優先パケットであることを示す情報を付加してもよく、また、ＩＰｖ６ヘッダのプライオリティフィールドに優先パケットであることを示す情報を付加してもよい。

パケット付加情報生成手段４１１にて生成されたパケット付加情報は、パケット化手段４０３に入力され、暗号化送信データに付加される。より具体的には、パケット付加情報は、ＴＣＰ／ＩＰまたはＵＤＰ／ＩＰプロトコルのヘッダの一部として暗号化送信データに付加され、送信パケットが生成される。

送信パケットには、また、ＡＫＥ手段４０２におけるＤＴＣＰ方式のコピー制御情報として、暗号化モード情報が付加される。

送信パケットは、さらに、フレーム化手段４０９においてＭＡＣヘッダが付加されて、イーサネット（Ｒ）フレームが生成され、イーサネット（Ｒ）フレームは、送信フレームとしてフレーム化手段４０９からネットワークに出力される。

なお、コンテンツのコピー制御情報をＣＧＩ（Ｃｏｐｙ Ｃｏｎｔｒｏｌ Ｉｎｆｏｒｍａｔｉｏｎ）、伝送における暗号化を表すコピー保護情報をＥＭＩ（Ｅｎｃｒｙｐｔｉｏｎ Ｍｏｄｅ Ｉｎｄｉｃａｔｏｒ）とよぶ。一般的には、ＥＭＩはＣＧＩと同等またはより強い保護モードが用いられる。

次に、パケット送受信装置４０１が受信フレームを受信する場合について説明する。

フレーム受信手段４１０は、ネットワークを介して受信フレームを受信する。フレーム受信手段４１０は、受信フレームに含まれるＭＡＣヘッダを抽出し、抽出したＭＡＣヘッダに基づいてフィルタリングを行い、フィルタリングによって得られたＩＰパケットをパケット受信手段４０５に出力する。

パケット受信手段４０５では、ＩＰパケットのＩＰパケットヘッダなどを識別することによって、フィルタリングを行い、パケット受信情報を生成する。フィルタリングによって、パケット受信情報として得られたＡＫＥ情報は、パケット受信手段４０５に含まれるパケット付加情報抽出手段４１２に入力される。パケット付加情報抽出手段４１２は、受信パケットからパケット付加情報を抽出し、抽出したパケット付加情報はＡＫＥ手段４０２に出力される。

このように、送信装置のＡＫＥ手段と、受信装置のＡＫＥ手段とは、ネットワークを介して１対１に接続することができるので、通信プロトコルを介してお互いにメッセージを交換することができる。

ＡＫＥ手段４０２は、パケット送受信装置４０１の位置情報と、送信パケットの到着先の位置情報または受信パケットの送信元の位置情報とが、あらかじめ決められた条件に合致する時に、認証を許可する。

ＡＫＥ手段４０２は、例えば、パケット送受信装置４０１と、送信パケットの到着先または受信パケットの送信元との間で、パケット送受信装置４０１から送信パケットの到着先または受信パケットの受信元までの片道または往復の伝播時間があらかじめ決められた制限時間より短い時間である場合に、認証を許可する。

あるいは、ＡＫＥ手段４０２は、パケット送受信装置４０１と、送信パケットの到着先または受信パケットの送信元との間の送受信区間において無線伝送区間が存在する場合、無線伝送区間ではデータをスクランブルして伝送するモードであることを確認する場合に、認証を許可してもよい。

したがって、二つのＡＫＥ手段の設定手順に従い、認証および鍵交換を実行することができる。

送信装置として機能するパケット送受信装置と、受信装置として機能するパケット送受信装置との間で認証および鍵交換が成立した後、送信装置は、暗号化したＡＶデータを送信する。

送信装置としては、ＭＰＥＧ－ＴＳデータが暗号化手段４０６に入力され、暗号化手段４０６は、ＭＰＥＧ－ＴＳを暗号化した暗号化ＭＰＥＧ－ＴＳデータを生成する。この暗号化ＭＰＥＧ－ＴＳデータは、パケット化手段４０３に入力され、パケット化手段４０３においてＴＣＰ／ＩＰプロトコルのヘッダが付加されて、送信パケットが生成される。

フレーム化手段４０９では、８０２．１Ｑ（ＶＬＡＮ）方式を用いて、送信パケットにさらにＭＡＣヘッダが付加されて、イーサネット（Ｒ）フレームに変換され、送信フレームが生成される。このように生成された送信フレームは、ネットワークに出力される。

ここで、ＭＡＣヘッダ内のＴＣＩ（Ｔａｇ　Ｃｏｎｔｒｏｌ　Ｉｎｆｏｒｍａｔｉｏｎ）内のＰｒｉｏｒｉｔｙ（ユーザ優先度）を高く設定することにより、ネットワーク伝送の優先度を一般のデータよりも高くすることができる。

受信装置では、ネットワークより入力する信号がフレーム受信手段４１０でＭＡＣヘッダを元にフィルタリングされ、ＩＰパケットとしてパケット受信手段４０５に入力される。パケット受信手段４０５でパケットヘッダなどの識別によりフィルタリングされ、復号手段４０７に入力され、復号されたＭＰＥＧ－ＴＳが出力される。

なお、送信条件設定管理手段４０４には、受信条件設定管理手段４０８から受信条件設定情報として、受信状況を送信装置にフィードバックするための情報が入力され、送信条件設定管理手段４０４は、これに基づいて、送信条件設定情報を生成し、送信条件設定情報に基づいて、パケット化手段４０３およびフレーム化手段４０９で生成するヘッダおよびペイロードが設定される。

図５は、ＭＰＥＧ－ＴＳを用いてパケット、さらには、フレームを生成して、

伝送する場合のパケット形式の一例を示す模式図である。ここで、ＭＰＥＧ－ＴＳは、ＩＳＯ／ＩＢＣ　１３８１８に準拠している。また、ＭＰＥＧ－ＴＳは、ＡＲＩＢ規格、ＡＲＩＢ　ＴＲ－Ｂ１４、ＡＲＩＢ　ＴＲ－Ｂ１５、または、ＡＲＩＢ　ＳＴＤ－Ｂ２１に基づく信号形式でもよい。

入力ストリームとして入力されるＭＰＥＧ－ＴＳは、１８８バイト毎に分断され、１８８バイトのＭＰＥＧ－ＴＳには６バイトのタイムコード（ＴＣ（Ｔｉｍｅ　Ｃｏｄｅ）が付加されて、１９４バイトの単位が形成される。ここで、ＴＣは、４２ビットのタイムスタンプと６ビットのベースクロックＩＤ（ＢＣＩＤ（Ｂａｓｅ　Ｃｌｏｃｋ　ＩＤ））とを含んでいる。

ＢＣＩＤによって、タイムスタンプの周波数情報を表すことができる。

例えば、

（ケース１）ＢＣＩＤが０ｘ００の場合は、タイムスタンプの周波数情報はない、

（ケース２）ＢＣＩＤが０ｚ０１の場合は、タイムスタンプの周波数情報としては２７ＭＨｚ（ＭＰＥＧ２のシステムクロック周波数）である、

（ケース３）また、ＢＣＩＤが０ｘ０２の場合は、タイムスタンプの周波数情報としては９０ｋＨｚ（ＭＰＥＧ１で使用されるクロック周波数）である、

（ケース４）ＢＣＩＤが０ｘ０３の場合は、タイムスタンプの周波数情報としては２４．５７６ＭＨｚ（ＩＥＥＥ　１３９４で使用されるクロック周波数）である、

（ケース５）ＢＣＩＤが０ｘ０４の場合は、タイムスタンプの周波数情報としては１００ＭＨｚ（イーサネット（Ｒ）で使用される周波数）である。

１９４バイト単位のデータを２つあわせて暗号化して暗号化データが生成され、さらに、その暗号化データに７バイトのパケット付加情報を付加すると、ＲＴＰプロトコルのペイロードが形成される。

ここでは、パケット付加情報は、２ビットのＥＭＩ（Ｅｎｃｒｙｐｔｉｏｎ　Ｍｏｄｅ　Ｉｎｄｉｃａｔｏｒ）と、１ビットのＯ／Ｅ（Ｏｄｄ／Ｅｖｅｎ）と

１３ビットのＲｅｓｅｒｖｅｄ　Ｄａｔａと、４０ビットのタイムスタンプまたは位置情報を含んでいる。ＥＭＩおよびＯ／ＥはＤＴＣＰ方式で規定されている。なお、Ｏ／Ｅの代わりに、ＤＴＣＰのシード情報（Ｎｃ）を用いてもよい。

パケット付加情報生成手段４１１（図４参照）が、ＡＫＥ関連情報を用いて、ＥＭＩおよびＯ／Ｅを生成する。

タイムスタンプまたは位置情報は、送信条件設定情報を用いてパケット付加情報生成手段４１１（図４参照）にて生成された情報であり、Ｒｅｓｅｒｖｅｄ　Ｄａｔａの後に続けて配置されている。タイムスタンプまたは位置情報は、また、Ｏ／ＥとＲｅｓｅｒｖｅｄ　Ｄａｔａとの間に配置されてもよい。

位置情報は、例えば、地域コード、住所、郵便番号、または、経度・緯度により範囲が指定された情報である。

ここでは、パケット付加情報は７バイトであったが、パケット付加情報は７バイトに限定されるものではない。

パケット付加情報は、タイムスタンプまたは位置情報を含んでなくてもよい。その場合、パケット付加情報は、２バイトとなる。

暗号化データに７バイトのパケット付加情報を付加すると、ＲＴＰプロトコルのペイロードが形成され、ヘッダとしてＲＴＰヘッダが付加されると、ＲＴＰプロトコルが形成される。

ＲＴＰプロトコルは、ＴＣＰパケットまたはＵＤＰパケットのペイロードであり、ヘッダとして、ＴＣＰヘッダまたはＵＤＰヘッダが付加されると、ＴＣＰパケットまたはＵＤＰパケットが形成される。

ＴＣＰパケットまたはＵＤＰパケットは、ＩＰパケットのペイロードであり、ヘッダとしてＩＰヘッダが付加されると、ＩＰパケットが生成される。ここで、ＩＰヘッダは、ＩＥＴＦでＩＰｖ４またはＩＰｖ６として規定されている。

さらにこのＩＰパケットはＭＡＣフレームのペイロードであり、ヘッダとしてイーサネットヘッダが付加されると、イーサネットパケットが生成される。

イーサネット（R）ヘッダとしては、図５に示すように、標準的なイーサネット（R）ヘッダとＩＥＥＥ　８０２．１Ｑ（ＶＬＡＮ）により拡張されたイーサネット（R）ヘッダの両方が適用可能である。

標準的なイーサネットヘッダは１４バイトであり、６バイトのＤＡ（Ｄｅｓｔｉｎａｔｉｏｎ　Ａｄｄｒｅｓｓ）と、６バイトのＳＡ（Ｓｏｕｒｃｅ　Ａｄｄｒｅｓｓ）と、２バイトの長さ／タイプを示す情報とを含む。

８０２．１Ｑで拡張されたイーサネットヘッダは１８バイトあり、８０２．１Ｑで拡張されたイーサネットヘッダは、ＳＡと長さ／タイプを示す情報との間に４バイトの８０２．１ｑ拡張部が設けられている点で標準的なイーサネットヘッダと異なる。

８０２．１ｑ拡張部は、２バイトのＴＰＩＤ（Ｔａｇ　Ｃｏｎｔｒｏｌ　ＩＤ）と、ＶＬＡＮ優先度を示す２バイトのＴＣＩ（Ｔａｇ　Ｃｏｎｔｏｒｏｌ　Ｉｎｆｏｒｍａｔｉｏｎ）とを含む。

ＴＣＩは、３ビットのＰｒｉｏｒｉｔｙ（Ｕｓｅｒ　Ｐｒｉｏｒｉｔｙ）と、１ビットのＣＦＩ（Ｃａｎｏｎｉｃａｌ　Ｆｏｒｍａｔ　Ｉｎｄｉｃａｔｏｒ）と、１２ビットのＶＩＤ（ＶＬＡＮ　Ｉｄｅｎｔｉｆｉｅｒ）とを含む。

Ｐｒｉｏｒｉｔｙの使用法は、ＩＳＯ／ＩＥＣ　１５８０２－３で規定されており、このＰｒｉｏｒｉｔｙのフラグを用いて、イーサネット（R）フレームの優先度を設定することができる。

次に、図６のプロトコルスタックを参照して上記手順を更に詳細に説明する。

図６は、本発明の実施の形態１によるプロトコルスタックを説明するための模式図である。

図６の左端には、ＯＳＩ（Ｏｐｅｎ　Ｓｙｓｔｅｍｓ　Ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ）モデルの階層を示している。この階層は、下層から順に、リンク層、ネットワーク層、トランスミッション層、アプリケーション層となっている。

まず、送信装置から受信装置に暗号化データがデータポートを介して、また、

データのＡＫＥ関連情報がＡＫＥポートを介して送信される。

受信装置では、データのコピー保護情報を解析して、認証方式を決定し、認証要求を送信装置に送る。

次に、送信装置では、乱数が発生され、この乱数を所定の関数に入力し、交換鍵を作成する。交換鍵の情報を所定の関数に入力すると、認証鍵が生成される。

受信装置でも所定の処理を行うことによって認証鍵が生成され、それにより、送信装置および受信装置は認証鍵を共有する。

なお、ここで暗号化を行うために使用する情報は、例えば、送信装置の独自情報（機器ＩＤ、機器の認証情報、マックアドレスなど）、秘密鍵、公開鍵、外部から与えられた情報などを１つ以上組み合わせて生成した情報であり、ＤＥＳ方式またはＡＥＳ方式などの暗号化強度の強い暗号化方式を用いることによって、強固な暗号化が可能である。

次いで、送信装置は認証鍵を用いて交換鍵を暗号化して暗号化交換鍵を生成し、暗号化交換鍵を受信装置に送信する。受信装置は、認証鍵を用いて、暗号化交換鍵を交換鍵に復号する。また、交換鍵と初期鍵更新情報を所定の関数に入力し、暗号化鍵（復号鍵）を生成する。

なお、送信装置は、暗号化鍵を時間的に変化させるために、時間とともに変更する鍵更新情報を生成し、この鍵更新情報を受信装置に送信する。

送信装置では、コンテンツデータであるＭＰＥＧ－ＴＳは暗号化鍵により暗号化され、暗号化データが生成される。そして暗号化データは、前述したＥＭＩ、Ｏ／ＥとともにＡＶデータとしてＴＣＰ（またはＵＤＰ）パケットのペイロードとなり、ＴＣＰ（またはＵＤＰ）パケットが生成される。さらにこのＴＣＰ（またはＵＤＰ）パケットはＩＰパケットのペイロードとして使用され、ＩＰパケットが生成される。さらにこのＩＰパケットはＭＡＣフレームのペイロードとして使用され、イーサネット（Ｒ）ＭＡＣフレームが生成される。

なお、ＭＡＣは、イーサネット（Ｒ）の規格であるＩＥＥＥ　８０２．３規格

だけでなく、無線ＬＡＮの規格であるＩＥＥＥ　８０２．１１規格のＭＡＣにも適用できる。

イーサネット（Ｒ）ＭＡＣフレームは、イーサネット（Ｒ）上を送信装置から受信装置に伝送される。受信装置は、所定の手順に従って暗号化鍵（復号鍵）を生成する。そして、受信したイーサネット（Ｒ）ＭＡＣフレームからＩＰパケットをフィルタリングする。さらにＩＰパケットからＴＣＰ（またはＵＤＰ）パケットを抽出する。そして、ＴＣＰ（またはＵＤＰ）パケットからＡＶデータを抽出し、交換鍵と鍵変更情報を用いて生成された暗号化鍵（復号鍵）により、データ（ＭＰＥＧ－ＴＳ）が復号される。

ＡＫＥ手段４０２が復号鍵を更新するタイミングを示すタイミング情報は、送信パケットに付加されていることが好ましい。その場合、ＡＫＥ手段４０２が復号鍵を更新するタイミングは、送信パケットのＴＣＰポート番号、またはＵＤＰポート番号を変化させることによって通知されてもよい。

送信パケットがＨＴＴＰを使用している場合、ＡＫＥ手段４０２が復号鍵を更新するタイミングは、ＨＴＴＰリクエスト毎に更新されるか、または、一定のデータ量毎に変化されてもよい。

あるいは、送信パケットがＲＴＰを使用している場合、ＡＫＥ手段４０２が復号鍵を更新するタイミングは、予め決められた期間（例えば、６０秒）内に更新されてもよい。

以上のように、ＭＰＥＧ－ＴＳなどのデータを送信装置で暗号化して、ＨＴＴＰ／ＴＣＰ／ＩＰまたはＲＴＰ／ＵＤＰ／ＩＰなどにより、ＩＰパケットをネットワークを介して伝送し、受信装置で元のデータに復号することが可能である。なお、前述したＯ／Ｅまたはシード情報（Ｎｃ）は、一定の規則、例えば、ＨＴＴＰリクエスト毎、または、一定量のＡＶデータ毎（例えば、１ＭＢ毎）、あるいは、予め決められた一定時間内に更新すると、よりセキュリティを向上させることができる。

ここで、再び図３を参照して、スイッチングハブを用いたネットワークトポロジーを変更することにより、ストリーム伝送とファイル転送を共存させることができることを説明する。

例えば、１階と２階との間のネットワーク３０５のデータレートを１００Ｍｂｐｓから１Ｇｂｐｓに拡張することによって、１階のＰＣと２階のＰＣとの間でのファイル転送を行いながら、同時に、１階のＤＶＤレコーダ、ＰＣまたはＴＶと、２階のＤＶＤレコーダ、ＰＣまたはＴＶとの間でＭＰＥＧ－ＴＳを暗号化してリアルタイムで伝送することができる。

例えば、８つの１００Ｍｂｐｓのポートと、１つの１Ｇｂｐｓのポートとを有する、市販されているスイッチングハブを用い、１階のネットワーク構成３０１と、２階のネットワーク構成３０２とを接続するネットワーク３０５に１Ｇｂｐｓのポートを接続し、残りの８つの１００ＭｂｐｓのポートにテレビなどのＡＶ機器を接続する。１００Ｍｂｐｓのポートは８つなので、８つのポートにデータがそれぞれ最大１００Ｍｂｐｓで入力されて１つのポートから出力される場合であっても、入力ポートの合計データレートは１００Ｍｂｐｓ×８ｃｈ＝８００Ｍｂｐｓであり、１Ｇｂｐｓより小さいため、８つの入力ポートから入力されたデータはスイッチングハブ内部で失われることなく、全て１Ｇｂｐｓの出力ポートから出力される。

したがって、１階のＡＶ機器から出力されるデータの全てを、ネットワーク３０５を介して、２階に伝送することが可能である。また、反対に、２階のＡＶ機器から出力されるデータの全てを、ネットワーク３０５を介して１階に伝送することが可能である。

以上のようなスイッチングハブを用いることによって、データのリアルタイム伝送とファイル転送とを同時に行うことができる。

（実施の形態２）

図７は、本発明の実施の形態２によるパケット送受信装置４０１Ａのブロック図である。

パケット送受信装置４０１Ａは、送信キュー制御手段６０１と、第１のキュー手段６０２と、第２のキュー手段６０３とをさらに備える点を除いて、実施の形態１において図４を参照して説明したパケット送受信装置４０１と同様の構成を有している。以下の説明では、説明を簡略化する目的で、主に、送信キュー制御手段６０１と、第１のキュー手段６０２と、第２のキュー手段６０３について説明する。

パケット化手段４０３は、一般データにＴＣＰ／ＩＰプロトコル処理をして、第１のパケットを生成し、第１のパケットを第１のキュー手段６０２に出力する。ここで、一般データとは、例えば、送信条件設定情報およびＡＫＥ関連情報である。

第１のキュー手段６０２は、第１のパケットを一時的に蓄積する。

パケット化手段４０３は、また、暗号化手段４０６にて生成された暗号化送信データにＴＣＰ／ＩＰプロトコル処理をして、第２のパケットを生成し、第２のパケットを第２のキュー手段６０３に出力する。

第２のキュー手段６０３は、第２のパケットを一時的に蓄積する。

ここで、パケット化手段４０３は、一般データを用いて第１のパケットを生成しているのに対し、コンテンツデータである暗号化送信データを用いて第２のパケットを生成している。

送信キュー制御手段６０２は、送信条件設定情報に基づいて、第１のキュー手段６０２と第２のキュー手段６０３とにパケットが一時的に蓄積されている場合に、どちらのパケットを優先的に出力するかを制御する。

具体的には、送信キュー制御手段６０１は、第１のパケットまたは第２のパケットの送信経路に関する情報と、第１のパケットまたは第２のパケットを送信するのに必要な帯域幅に関する情報と、送信パケットの送信から到着までの遅延に

関する情報と、第１のパケットまたは第２のパケットの優先度に関する情報とのうち少なくとも１つの情報を用いて、第１のキュー手段に蓄積された第１のパケットおよび第２のキュー手段に蓄積された第２のパケットのいずれを送信するかを制御する。

送信キュー制御手段６０２は、通常状態では、一般データよりもＭＰＥＧ－ＴＳなどのコンテンツデータを優先的に出力するように第１のキュー手段６０２および第２のキュー手段６０３を制御する。すなわち、送信キュー制御手段６０２は、コンテンツデータである暗号化送信データを、一般データよりも優先させる優先データとして取り扱う。

優先データは、例えば、ＭＰＴＥ　２５９Ｍ規格で規定された非圧縮ＳＤ方式信号、または、ＳＭＰＴＥ　２９２Ｍ規格で規定された非圧縮ＨＤ形式、または、ＩＥＣ　６１８８３規格で規定されたＩＥＥＥ１３９４によるＤＶまたはＭＰＥＧ－ＴＳの伝送ストリーム形式、または、ＤＶＢ規格Ａ０１０で規定されたＤＶＢ－ＡＳＩによるＭＰＥＧ－ＴＳ形式、ＭＰＥＧ－ＰＳ形式、ＭＰＥＧ－ＥＳ形式、ＭＰＥＧ－ＰＥＳ形式の内の少なくとも一つのデータストリーム形式である。

送信キュー制御手段６０１は、ＩＥＴＦ　ｒｆｃ２２０５、ｒｆｃ２２０８、ｒｆｃ２２０９で記載されたＲＳＶＰ方式、ＩＥＴＦ　ｒｆｃ２２１０、ｒｆｃ２２１１、２２１２，ｒｆｃ２２１５で記載されたＩｎｔｓｅｒｖ方式、ＩＥＴＦ　ｒｆｃ２４７４、ｒｆｃ２４７５、ｒｆｃ２５９７、ｒｆｃ２５９８で記載されたＤｉｆｆｓｅｒｖ方式のいずれか１つの制御方式を使用してもよい。

フレーム化手段４０９は、第１のキュー手段６０２または第２のキュー手段６０３からそれぞれ出力された第１のパケットまたは第２のパケットを用いて、送信フレームを生成し、ネットワークに送信フレームを出力する。

送信キュー制御手段６０１は、第１のキュー手段６０２から送信される第１のパケットと第２のキュー手段６０３から送信される第２のパケットとの間隔を平均化するように第１のキュー手段および第２のキュー手段を制御してもよい。

一般的に、送信装置から受信装置にＭＰＥＧ－ＴＳを低遅延で伝送する場合には、ＭＰＥＧ－ＴＳのためのバッファも小さいため、オーバーフローが発生しやすい。

送信装置において、ＭＰＥＧ－ＴＳのためのバッファ（例えば、第２のキュー手段６０３のバッファ）がオーバーフローしそうになった場合、あるいは、受信装置からフィードバックされた情報を参照して受信装置のＭＰＥＧ－ＴＳのためのバッファがアンダーフローしそうになったことが判明した場合には、ＭＰＥＧ－ＴＳのデータを優先的に出力するように第２のキュー手段６０３の優先度を更に適応的に上げることにより、このようなバッファの破綻を回避することができる。

送信装置が受信装置を遠隔操作する場合において、受信装置の再生、停止などの制御応答をより速くするためには、送信装置において第１のキュー手段６０２の優先度を適応的に上げればよい。しかしながら、この場合には、ＭＰＥＧ－ＴＳのためのバッファがオーバーフロまたはアンダーフローする可能性がある。

したがって、バッファのオーバーフローおよびアンダーフローを避け、かつ、受信装置の再生、停止などの制御応答をより速くするように送信装置が受信装置を遠隔操作するための態様としては、受信装置を遠隔制御するためのパケットをキュー手段を経由することなく、パケット化手段４０３から直接フレーム化手段４０９に出力することにより、迅速な制御応答を実現することができる。あるいは、受信装置を遠隔制御するためのパケットに対して第３のキュー手段を新たに設けることにより、迅速な制御応答を実現することができる。

受信装置の動作は実施の形態１と同様である。

送信キュー制御手段６０１は、第２のパケットのデータレートが所定の値より小さくならないように、第１のキュー手段６０２および第２のキュー手段６０３を制御することが好ましい。また、送信キュー制御手段６０１は、第２のキュー手段６０３に蓄積される時間があらかじめ決めた値より常に小さくなるように、

送信キュー制御手段６０１は第１のキュー手段６０２および第２のキュー手段６０３を制御することが好ましい。

（実施の形態３）

実施の形態３について説明する。

図８は、本発明の実施の形態３によるパケット送受信装置４０１Ｂのブロック図である。

パケット化手段４０３が、第１のパケット化手段７０１と、第２のパケット化手段７０２とを含み、パケット受信手段４０５が、第１のパケット受信手段７０３と、第２のパケット受信手段７０４とを含む点を除いて、パケット送受信装置４０１Ｂは、実施の形態２において図７を参照して説明したパケット送受信装置４０１Ａと同様の構成を有している。以下の説明では、説明を簡略化する目的で、主に、第１のパケット化手段７０１と、第２のパケット化手段７０２と、第１のパケット受信手段７０３と、第２のパケット受信手段７０４とについて説明する。

はじめに、この送受信装置４０１Ｂが送信フレームを送信する場合について説明する。

第１のパケット化手段７０１は、例えば、プロセッサーを含んでおり、第１のパケット化手段７０１には、送信条件設定管理手段４０４にて生成された送信条件設定情報およびＡＫＥ関連情報が入力される。第１のパケット化手段７０１は、プロセッサーを用いたソフトウエア処理で送信条件設定情報およびＡＫＥ関連情報をＴＣＰ／ＩＰプロトコル処理することによって、第１のパケットを生成する。第１のパケット化手段７０１は、第１のパケットを第１のキュー手段６０２に出力する。

第１のパケット化手段７０１は、ＩＥＴＦ文書で規定されているデータ処理プロトコルであるＲＴＣＰ，ＲＴＳＰ，ＨＴＴＰ、ＴＣＰ、ＵＤＰ、ＩＰのうちの少なくとも１つのヘッダを付加する。

第２のパケット化手段７０２には、ＭＰＥＧ－ＴＳなどの送信データを暗号化手段４０６にて暗号化した暗号化送信データが入力される。第２のパケット化手段７０２にはＡＫＥ関連情報が入力されてもよい。ＡＫＥ関連情報は、例えば、コピー制御情報、暗号化鍵更新情報である。

第２のパケット化手段７０２はハードウエア処理によって、この暗号化送信データをＵＤＰ／ＩＰプロトコル処理することによって、第２のパケットを生成する。第２のパケット化手段７０２は、第２のパケットを第２のキュー手段６０３に出力する。

第２のパケット化手段７０２は、データにシーケンス番号を付加するか、または、ＩＥＴＦ文書で規定されているデータ処理プロトコルであるＲＴＰ，ＵＤＰ、ＨＴＴＰ、ＴＣＰ、ＩＰのうちの少なくとも１つのヘッダを付加する。

送信キュー制御手段６０１は、第１のキュー手段６０２と第２のキュー手段６０３との両方にパケットが一時的に蓄積されている場合、上述した実施の形態２と同様に、第１のキュー手段６０２および第２のキュー手段６０３のうちのどちらのパケットを優先的に出力するかを制御する。

この送受信装置４０１Ｂが受信フレームを受信する場合について説明する。

フレーム受信手段４１０は、ネットワークを介して、受信フレームを受信する。フレーム受信手段４１０は、フレーム受信手段４１０を、ＭＡＣヘッダに基づいて受信フレームからＩＰパケットをフィルタリングする。

ここで、ＩＰパケットが、第１のパケット化手段７０１にて生成される第１のパケットと同様のパケットである場合、そのＩＰパケットは第１のパケット受信手段７０３に入力され、ＩＰパケットが、第２のパケット化手段７０２にて生成される第２のパケットと同様のパケットである場合、そのＩＰパケットは第２のパケット受信手段７０４に入力される。

第１のパケット受信手段７０３ではプロセッサーを用いたソフトウエア処理でＴＣＰ／ＩＰプロトコルの受信処理を行い、この処理によって生成されたパケッ

ト受信情報をＡＫＥ手段４０２または受信条件設定管理手段４０８に出力する。

また、第２のパケット受信手段７０４ではハードウエア処理によりＵＤＰ／ＩＰプロトコルの受信処理を行い、この処理によって抽出された受信データを復号手段４０７に出力する。復号手段４０７では、受信データの暗号が復号される。

次に、図９のプロトコルスタックを用い、上記手順を更に詳細に説明する。

図９は、本発明の実施の形態３によるプロトコルスタックを説明するための模式図である。

図９に示すプロトコルスタックは、ＭＰＥＧ－ＴＳなどのＡＶデータのトランスミッション層がＵＤＰである点を除いて、図６を参照して説明したプロトコルスタックと同様の構成である。したがって、以下の説明では、主にトランスミッション層がＵＤＰである点について説明する。

送信装置において、コンテンツである送信データ（例えば、ＭＰＥＧ－ＴＳ）を暗号化鍵Ｋｃを用いて暗号化することによって、暗号化送信データが生成される。暗号化送信データは、前述したＥＭＩ、Ｏ／ＥとともにＡＶデータとして、ハードウエアによりＵＤＰパケットのペイロードとなり、ＵＤＰヘッダを付加することによってＵＤＰパケットが生成される。さらにこのＵＤＰパケットはＩＰパケットのペイロードとして使用され、ＩＰヘッダを付加することによって、ＩＰパケットが生成される。

なお、送信装置から受信装置への、ＥＭＩおよびＯ／Ｅを伝送する方法としては、例えば、専用の別パケットを生成して伝送することも可能である。その場合、暗号化鍵の復号がさらに困難となり、コンテンツの盗聴、漏洩をより困難にできる。インターネットなどの公衆網においても、リアルタイムに伝送されるＡＶデータの暗号化パラメータを変化させたり、別パケットとして送ることによって、コンテンツの盗聴、漏洩をより困難にすることができる。

管理制御データに関しては図６の例と同様に、ソフトウエア処理によりＴＣＰパケットが生成され、ＩＰパケットが生成される。

イーサネット（R）ＭＡＣフレームは、イーサネット（R）上を送信装置から受信装置に伝送される。受信装置では、所定の手順に従って暗号化鍵を生成する。そして、受信したイーサネット（R）ＭＡＣフレームからＩＰパケットがフィルタリングされる。さらにＩＰパケットからＵＤＰパケットが抽出され、ＵＤＰパケットから受信データが抽出され、暗号化鍵Ｋｃを用いて、受信データ（例えば、ＭＰＥＧ－ＴＳ）が復号される。

このように、暗号化送信データおよび一般データが処理されるレイヤよりも下位レイヤの受信フレームを処理するレイヤにおいて、受信フレームに含まれる受信パケットの通信プロトコルヘッダから優先データと一般データを選別して、優先データの処理と一般データの処理を独立に行うことができる。

図１０は、ＭＰＥＧ－ＴＳを用いてパケット、さらには、フレームを生成して、、伝送する場合のパケット形式の一例を示す模式図である。ここでも、ＭＰＥＧ－ＴＳは、ＩＳＯ／ＩＢＣ　１３８１８に準拠している。

入力ストリームとして入力されるＭＰＥＧ－ＴＳは、１８８バイト毎に分断され、１８８バイトのＭＰＥＧ－ＴＳには６バイトのタイムコード（ＴＣ（Ｔｉｍｅ　Ｃｏｄｅ）を付加されて、１９４バイトの単位が形成される。ここで、ＴＣは、４２ビットのタイムスタンプと６ビットのベースクロックＩＤ（ＢＣＩＤ（Ｂａｓｅ　Ｃｌｏｃｋ　ＩＤ））とを含んでいる。

ＢＣＩＤによって、タイムスタンプの周波数情報を表すことができる。

例えば、

（ケース１）ＢＣＩＤが０ｘ００の場合は、タイムスタンプの周波数情報はない、

（ケース２）ＢＣＩＤが０ｚ０１の場合は、タイムスタンプの周波数情報としては２７ＭＨｚ（ＭＰＥＧ２のシステムクロック周波数）である、

（ケース３）また、ＢＣＩＤが０ｘ０２の場合は、タイムスタンプの周波数情報としては９０ｋＨｚ（ＭＰＥＧ１で使用されるクロック周波数）である、

（ケース４）ＢＣＩＤが０ｘ０３の場合は、タイムスタンプの周波数情報として

は２４．５７６ＭＨｚ（ＩＥＥＥ　１３９４で使用されるクロック周波数）である、

（ケース５）ＢＣＩＤが０ｘ０４の場合は、タイムスタンプの周波数情報としては１００ＭＨｚ（イーサネット（Ｒ）で使用される周波数）である。

１９４バイト単位のデータを２つあわせて暗号化して暗号化データが生成され、さらに、その暗号化データに２バイトのパケット付加情報を付加すると、ＲＴＰプロトコルのペイロードが形成される。

ここでは、パケット付加情報は、２ビットのＥＭＩ（Ｅｎｃｒｙｐｔｉｏｎ　Ｍｏｄｅ　Ｉｎｄｉｃａｔｏｒ）と、１ビットのＯ／Ｅ（Ｏｄｄ／Ｅｖｅｎ）と１３ビットのＲｅｓｅｒｖｅｄ　Ｄａｔａと、４０ビットのタイムスタンプまたは位置情報を含んでいる。ＥＭＩおよびＯ／ＥはＤＴＣＰ方式で規定されている。なお、Ｏ／Ｅの代わりに、ＤＴＣＰのシード情報（Ｎｃ）を用いてもよい。

パケット付加情報生成手段４１１（図４参照）が、ＡＫＥ関連情報を用いて、ＥＭＩおよびＯ／Ｅを生成する。

タイムスタンプまたは位置情報は、送信条件設定情報を用いてパケット付加情報生成手段４１１（図４参照）にて生成された情報であり、Ｒｅｓｅｒｖｅｄ　Ｄａｔａの後に続けて配置されている。タイムスタンプまたは位置情報は、また、Ｏ／ＥとＲｅｓｅｒｖｅｄ　Ｄａｔａとの間に配置されてもよい。

位置情報は、例えば、地域コード、住所、郵便番号、または、経度・緯度により範囲が指定された情報である。

ここでは、パケット付加情報は７バイトであったが、パケット付加情報は７バイトに限定されるものではない。

パケット付加情報は、タイムスタンプまたは位置情報を含んでなくてもよい。その場合、パケット付加情報は、２バイトとなる。

暗号化データに７バイトのパケット付加情報を付加すると、ＲＴＰプロトコルのペイロードが形成され、ヘッダとしてＲＴＰヘッダが付加されると、ＲＴＰプ

ロトコルが形成される。

ＲＴＰプロトコルは、ＴＣＰパケットまたはＵＤＰパケットのペイロードであり、ヘッダとして、ＴＣＰヘッダまたはＵＤＰヘッダが付加されると、ＴＣＰパケットまたはＵＤＰパケットが形成される。

ＴＣＰパケットまたはＵＤＰパケットは、ＩＰパケットのペイロードであり、ヘッダとしてＩＰヘッダが付加されると、ＩＰパケットが生成される。

さらにこのＩＰパケットはＭＡＣフレームのペイロードであり、ヘッダとしてイーサネットヘッダが付加されると、イーサネットパケットが生成される。

イーサネット（Ｒ）ヘッダとしては、図１０に示す様に、標準的なイーサネット（Ｒ）ヘッダとＩＥＥＥ　８０２．１Ｑ（ＶＬＡＮ）により拡張されたイーサネット（Ｒ）ヘッダのと両方が適用可能である。

標準的なイーサネットヘッダは１４バイトであり、６バイトのＤＡ（Ｄｅｓｔｉｎａｔｉｏｎ　Ａｄｄｒｅｓｓ）と、６バイトのＳＡ（Ｓｏｕｒｃｅ　Ａｄｄｒｅｓｓ）と、２バイトで示される長さ／タイプを示す情報とを含む。

８０２．１Ｑで拡張されたイーサネットヘッダは１８バイトあり、８０２．１Ｑで拡張されたイーサネットヘッダは、標準的なイーサネットヘッダと、ＳＡと長さ／タイプを示す情報との間に４バイトの８０２．１ｑ拡張部が設けられている点で異なる。

８０２．１ｑ拡張部は、２バイトのＴＰＩＤ（Ｔａｇ　Ｃｏｎｔｒｏｌ　ＩＤ）と、ＶＬＡＮ優先度を示す２バイトのＴＣＩ（Ｔａｇ　Ｃｏｎｔｏｒｏｌ　Ｉｎｆｏｒｍａｔｉｏｎ）とを含む。

ＴＣＩは、３ビットのＰｒｉｏｒｉｔｙ（Ｕｓｅｒ　Ｐｒｉｏｒｉｔｙ）と、１ビットのＣＦＩ（Ｃａｎｏｎｉｃａｌ　Ｆｏｒｍａｔ　Ｉｎｄｉｃａｔｏｒ）と、１２ビットのＶＩＤ（ＶＬＡＮ　Ｉｄｅｎｔｉｆｉｅｒ）とを含む。

Ｐｒｉｏｒｉｔｙの使用法は、ＩＳＯ／ＩＥＣ　１５８０２－３で規定されており、このＰｒｉｏｒｉｔｙのフラグを用いて、イーサネット（Ｒ）フレームの

優先度を設定することができる。

以上により、送信装置と受信装置との間で送信データ（例えば、ＭＰＥＧ－ＴＳ）を暗号化してリアルタイム伝送が可能となる。また、第２のパケット化手段がハードウエアで構成されているため、本質的にソフトウエア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。これにより、全ての優先データパケットが完全に送信され、リアルタイム性の保証された高品質映像の伝送が可能となる。

また、一般データは一時的にバッファに蓄積され、優先データの伝送が優先的に行なわれる間に間欠的に伝送される。また、処理すべきデータ量の小さい第１のパケット化手段はマイコンなど安価なプロセッサで構成してもよい。

さらに、ハードウエア処理により、受信処理においても、イーサネット（Ｒ）フレームを受信して、３層のＩＰヘッダ、４層のＵＤＰヘッダを同時に検査することもできる。

また、優先データであるコンテンツデータ（例えば、ＭＰＥＧ－ＴＳ）のパケットと一般データのパケットとを分離し、コンテンツデータのパケットの処理をハードウェアで行うことにより、受信フレームの取りこぼしが発生せず、リアルタイム性が保証された高品質な受信を行うことができる。

パケットを送信するタイミング、または、２つのキュー手段からのパケットを送信する割合をソフトウェアではなくハードウェアで制御することによって、クロック単位で完全に送信を制御することが可能である。これにより全ての優先パケットが完全に送信され、リアルタイム性の保証された高品質の伝送が可能となる。また、出力パケットのシェイピングもクロック単位で正確に行われるため、初段のルータ、またはスイッチングハブでのパケット廃棄の発生確率が非常に少ない高品質な通信が可能となる。

（実施の形態４）

図１１は、本発明の実施の形態４によるパケット送受信装置４０１Ｃのブロック図を示す。

ＡＫＥ手段４０２が、ＤＴＣＰ情報生成手段１００１と、ＡＫＥコマンド受信処理手段１００２と、ＡＫＥコマンド送信処理手段１００３と、交換鍵生成手段１００４と、暗号化鍵生成手段１００５と、暗号化鍵変更情報生成手段１００６と、復号鍵生成手段１００７とを含む点を除いてパケット送受信装置４０１Ｃは、実施の形態４において図８を参照して説明したパケット送受信装置４０１Ｂと同様の構成である。したがって、以下の説明では、主に、ＤＴＣＰ情報生成手段１００１と、ＡＫＥコマンド受信処理手段１００２と、ＡＫＥコマンド送信処理手段１００３と、交換鍵生成手段１００４と、暗号化鍵生成手段１００５と、暗号化鍵変更情報生成手段１００６と、復号鍵生成手段１００７とについて説明する。

パケット送受信装置４０１Ｃにおいては、以下のステップに従ったＤＴＣＰ方式により暗号化送信データの送信が行なわれる。ここでは、パケットを送信するソースおよびパケットを受信するシンクの両方の機能を、パケット送受信装置４０１Ｃを参照して説明するが、これは、説明を簡略化するためであり、実際には、二つの異なるパケット送受信装置においてパケットの送受信が行われることに留意されたい。

（ステップ１）認証・鍵交換関連情報として、伝送時における暗号化送信データの暗号化状態を表すコピー保護情報がＤＴＣＰ情報生成手段１００１に入力される。

（ステップ２）まず、送信装置（ソース）においてデータの送信要求を発生させ、ＤＴＣＰ情報生成手段１００１からデータの保護モード情報（ＥＭＩ情報）が第１のパケット化手段７０１に出力され、送信パケットが生成され、送信パケットは送信装置から送信される。

（ステップ３）送信装置から送信された送信パケットは、受信装置（シンク）において、受信パケットとして受信され、ＡＫＥコマンド受信処理手段１００２

は、第１のパケット受信手段７０３から受け取ったデータのコピー保護情報を解析し、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、ＡＫＥ送信処理手段１００３を通じて認証要求を送信装置に送る。

（ステップ４）送信装置と受信装置との間でＤＴＣＰ方式の所定の処理が行なわれ、認証鍵が共有される。

（ステップ５）次に、送信装置はＡＫＥ送信処理手段１００３において、認証鍵を用いて交換鍵を暗号化することによって生成した暗号化交換鍵を第１のパケット化手段７０１を介して受信装置に送り、受信装置においてＡＫＥコマンド受信処理手段１００２によって暗号化交換鍵は抽出され、交換鍵生成手段１００４において交換鍵に復号される。

（ステップ６）送信装置では、暗号化鍵を時間的に変化させるために、暗号化鍵生成手段１００５において、時間とともに変更するシード情報（Ｏ／Ｅ）を生成し、シード情報は、ＤＴＣＰ情報生成手段１００１および第１のパケット化手段７０１を介して受信装置に送信される。

（ステップ７）送信装置では、暗号化鍵生成手段１００５において交換鍵とシード情報とを用いて暗号化鍵を生成して、暗号化手段４０６は、この暗号化鍵を用いて、送信データ（例えば、ＭＰＥＧ－ＴＳ）を暗号化して、暗号化送信データを生成し、暗号化手段４０６は、暗号化送信データを第２のパケット化手段７０２に出力する。

（ステップ８）受信装置では、暗号化鍵変更情報生成手段１００６は第１のパケット受信手段７０３からシード情報を受信し、復号鍵生成手段１００７はこのシード情報と交換鍵生成手段１００４の交換鍵とを用いて、暗号化鍵（復号鍵）を生成する。

（ステップ９）受信装置では、この暗号化鍵（復号鍵）を用いて復号手段４０７において、暗号化されたデータを復号する。

図１２は、パケット化手段４０３に含まれる第１のパケット化手段７０１およ

び第２のパケット化手段７０２、ならびに、パケット受信手段４０５に含まれる第１のパケット受信手段７０３および第２のパケット受信手段７０４におけるパケット処理について説明するためのブロック図である。

第１のパケット化手段７０１では、入力されたデータを、ＲＴＣＰまたはＲＴＳＰプロトコル、ＴＣＰまたはＵＤＰプロトコル、さらにはＩＰプロトコルに形成するための処理が順次なされる。

なお、ＲＴＣＰプロトコル（ｒｆｃ１８８９）を使用する場合には、ネットワークの実効帯域幅および遅延時間などといったネットワークの通信状態を受信装置より送信装置に送り、送信装置は送られてきたネットワークの通信状態に合わせてＲＴＰで送信するデータの品質を調整して送信することもできる。

また、ＲＴＳＰプロトコル（ｒｆｃ２３２６）は、再生、停止、早送りなどの制御コマンドを送ることもでき、ＡＶファイルからデータをダウンロードしながらデータを再生することが可能である。

第２のパケット化手段７０２では、入力されるデータをＲＴＰプロトコル、ＵＤＰプロトコル、そして、ＩＰプロトコルに形成するための処理がそれぞれ順次行われ、ＩＰパケットが生成される。

また、第１のパケット受信手段７０３では、フィルタリングなどのＩＰプロトコルの受信処理、ＴＣＰまたはＵＤＰプロトコルの受信処理、さらに、ＲＴＣＰまたはＲＴＳＰプロトコルの受信処理が順次行われ、それにより、受信パケットに含まれる受信データが抽出される。

また、第２のパケット受信手段７０４は、フィルタリングなどのＩＰプロトコルの受信処理、ＵＤＰプロトコルの受信処理、さらに、ＲＴＰプロトコルの受信処理が順次なされ、受信パケットに含まれる受信データが抽出される。

以上により、送信装置と受信装置との間でデータ（例えば、ＭＰＥＧ－ＴＳ）をＤＴＣＰ方式に基づいて暗号化し、リアルタイムな伝送が可能となる。また、第２のパケット化手段がハードウエアで構成されているため、本質的にソフトウ

エア処理に起因する送信パケットの送り残しおよび受信パケットの取りこぼしが発生しない。また、データ量の小さい第１のパケット化手段はマイコンなどの安価なプロセッサで構成することができる。

また、何らかの原因であらかじめ決められた条件に合致しないために受信装置と受信装置との認証が成立しない場合であっても、例えば、すでに送信装置または受信装置が記憶している証明書、ＭＡＣアドレスなどの情報および指紋、虹彩などの個人を特定する生体情報の少なくとも１つを用いて、送信装置と受信装置との認証をおこなってもよい。

再び、図１１を参照すると、認証・鍵交換手段４０２のＡＫＥコマンド受信処理手段１００２は、パケット送受信装置４０１Ｃと、送信パケットの到着先または受信パケットの送信元との間で認証を行った場合に、送信パケットの到着先または受信パケットの送信元に関する情報を一時的に記憶する記憶手段と、パケット送受信装置と、送信パケットの到着先または受信パケットの送信元とがあらかじめ決められた条件に合致しないために認証が成立しない場合に、記憶手段にて記憶された情報と、送信パケットの到着先に関する情報または受信パケットの送信先に関する情報とを照合し、パケット送受信装置と送信パケットの到着先または受信パケットの送信元との間で認証を行う、照合手段として機能してもよい。

これにより、例えば、家庭で相互認証を行った２つの機器を遠隔地間で特定認証可能となり、家庭と旅行先などの遠隔地との間でのデータコンテンツの伝送、データコンテンツのリモート伝送が可能となる。

（実施の形態５）

図１３は、パケット化手段４０３Ａの第１のパケット化手段７０１および第２のパケット化手段７０２Ａ、ならびに、パケット受信手段４０５Ａ内の第１のパケット受信手段７０３および第２のパケット受信手段７０４Ａにおけるパケット処理について説明するためのブロック図である。

パケット化手段４０３Ａおよびパケット受信手段４０５Ａは、第２のパケット化手段７０２、および、第２のパケット受信手段７０４Ａが異なる点を除いて、図１２を参照して説明したパケット化手段４０３およびパケット受信手段４０５と同様の構成である。したがって、以下の説明では、主に第２のパケット化手段７０２Ａ、および、第２のパケット受信手段７０４Ａについて説明する。

第２のパケット化手段７０２Ａは、入力されるデータに対してエラー訂正処理を行ない、ＲＴＰプロトコル、ＵＤＰプロトコル、そしてＩＰプロトコルを形成するようにそれぞれ順次的に処理することによって、ＩＰパケットを生成する。

また、第２のパケット受信手段７０４Ａは、フィルタリングなどのＩＰプロトコルの受信処理、ＵＤＰプロトコルの受信処理、ＲＴＰプロトコルの受信処理、さらにエラー訂正符号処理を順次的に行い、それにより、エラー訂正されたデータが出力される。

図１４は、本発明の実施の形態５によるプロトコルスタックを説明するための模式図である。

送信装置では、ＡＶデータにエラー訂正符号が付加され（ＥＣＣエンコード）、ＵＤＰプロトコルに渡される。また、受信装置では、ＵＤＰプロトコル処理よりデータを受け取りエラー訂正をして上位層のＡＶデータとなる。

エラー訂正方式の例を、図１５および図１６を参照して、以下に説明する。

図１５は、エラー訂正方式がリードソロモン方式である場合を説明するための模式図である。

図１６は、エラー訂正方式がパリティ方式である場合を説明するための模式図である。

ここでは、２つの単位のデータ（ＭＰＥＧ－ＴＳ）をエラー訂正インターリーブマトリックスに入力している。なお、各行にはシーケンス番号を２バイト使用している。

次いで、たとえば、２バイトのパケット付加情報を用いて、さらに、ＲＴＰヘ

ッダ、ＵＤＰヘッダ、ＩＰヘッダ、イーサネット（Ｒ）ヘッダを付加することによって、イーサネット（Ｒ）フレームを生成する。

このように、送信装置と受信装置との間でデータ（例えば、ＭＰＥＧ－ＴＳ）をＤＴＣＰ方式に基づいて暗号化し、さらにエラー訂正符号を付加して、リアルタイムに伝送することが可能となる。

また、第２のパケット化手段がハードウエアで構成されていると、本質的にソフトウエア処理に起因する送信パケットの送り残しおよび受信パケットの取りこぼしが発生しない。また、データ量の小さい第１のパケット化手段はマイコンなど安価なプロセッサで構成することができる。

（実施の形態６）

図１７は、本発明の実施の形態６によるパケット送受信装置４０１Ｄのブロック図である。

パケット送受信装置４０１Ｄでは、受信データ（例えば、ＭＰＥＧ－ＴＳなどのＡＶデータ）の受信機能を取り除いた点を除いて、図１１を参照して説明したパケット送受信装置４０１Ｃと同様の構成を有している。

図１８は、本発明の実施の形態６の別の形態によるパケット送受信装置４０１Ｅのブロック図である。

パケット送受信装置４０１Ｅは、送信データ（例えば、ＭＰＥＧ－ＴＳなどのＡＶデータ）の送信機能を取り除いた点を除いて、図１１を参照して説明したパケット送受信装置４０１Ｃと同様の構成を有している。

なお、このように、データの受信機能または送信機能を取り除くことは、実施の形態１から実施の形態５にて説明したすべてのパケット送受信装置に適用できる。また、本発明は、送信または受信のみを行う機器に対しても適用可能であり、それにより、低コスト化を図ることができる。

なお、上述した実施の形態１から６においては、一般のＩＰネットワークなど

パケットの順序性が保証されていない通信網で伝送する場合には、シーケンス番号を付加したパケットを送信し、受信装置にてパケットに付加されたシーケンス番号を用いて順序性の保証を行ってもよい。この順序性の保証は、ＯＳＩモデルの第４層以上、すなわち、ＲＴＰプロトコルまたはビデオ信号処理などで行なうことができる。

なお、送信装置においてハードウエア処理され、伝送されたＡＶデータのパケットは、ネットワークにおいてフラグメント化されることを防ぐことができる。具体的には、送信装置において、あらかじめアプリケーションレベルの処理で、通信網においてフラグメント化されない最大サイズ（ＭＴＵ）を検査し、それ以下のパケットサイズで伝送すればよい。

具体的には、送信条件設定管理手段４０４および受信条件設定管理手段４０８は、送信フレームの送信から到着するまでの間において送信パケットの送信先から受信先までの経路における最大伝送パケットサイズの検出を行ない、最大伝送パケットサイズ情報を用いて、送信条件設定情報または受信条件設定管理手段を生成してもよい。

あるいは、ＲＦＣの規格において、全ての端末は５７６バイトのサイズのＩＰパケットを取り扱えなければならないと規定されているので、ルータ等の多くのネットワーク機器ではこれ以下のＩＰパケットに対してフラグメント化が起こらない。したがって、ＩＰパケットのサイズが５７６バイト以下となるように、送信装置でハードウエア処理されるＡＶデータのパケットサイズを調整すればよい。なお、送信装置でハードウエア処理されるＡＶデータのパケットにフラグメント化が起こらない場合は、受信したパケットがフラグメント化されていれば全て一般パケットとして処理すればよい。なお、イーサネット（Ｒ）のＩＰパケットの最大値を越えた場合は送信装置においてフラグメント化する必要がある。したがって、優先パケットのフラグメント化を起こさせないためにはＩＰパケットの最大値以下でなければならないことは言うまでもない。

また、通信網においてフラグメント化が起こる確率が非常に低い場合は、送信装置でハードウエア処理され伝送されたＡＶデータのパケットのＩＰヘッダにフラグメント禁止のフラグを付して伝送することにより、ルータがフラグメントせざるを得ない状態ではＩＰパケットを廃棄させることにより、受信装置のフラグメント化処理負荷を軽減してもよい。この場合、非常に少数のパケットは損失となるが、受信装置で誤り訂正あるいは誤り修整を行うことで通信品質を補償することができる。

さらに、実施の形態１から６においては、通信網プロトコルの具体例としてイーサネット（Ｒ）を説明したが、本発明は、これに限定されるものではない。

また、ビデオ信号処理の例として、実施の形態１から６ではＭＰＥＧ－ＴＳを用いたが、本発明は、これに限定されるものではない。本発明の入力ストリームは、ＭＰＥＧ１／２／４などＭＰＥＧ－ＴＳストリーム（ＩＳＯ／ＩＥＣ　１３８１８）、ＤＶ（ＩＥＣ　６１８３４、ＩＥＣ　６１８８３）、ＳＭＰＴＥ　３１４Ｍ（ＤＶ－ｂａｓｅｄ）、ＳＭＰＴＥ　２５９Ｍ（ＳＤＩ）、ＳＭＰＴＥ　３０５Ｍ（ＳＤＴＩ）、ＳＭＰＴＥ　２９２Ｍ（ＨＤ－ＳＤＩ）等で規格化されているストリームを含んだあらゆる映像、音声に関するストリームまでも適用可能である。

映像または音声のデータレートは、ＣＢＲ（ｃｏｎｓｔａｎｔ　ｂｉｔ　ｒａｔｅ）に限定されるものではない。ＶＢＲ（ｖａｒｉａｂｌｅ　ｂｉｔ　ｒａｔｅ）でもよい。さらに、映像または音声だけでなく、一般のリアルタイムデータ、あるいは優先的に送受信を行うデータであればどのようなものでも本発明から排除されるべきではない。

また、本発明で使用されるデータは、ファイルであってもよい。データがファイルである場合、送信装置と受信装置との間の伝播遅延時間と、送信装置および受信装置の処理能力との関係により、一定の条件下でリアルタイムよりも高速に伝送することも可能である。

また、インターネットの分野で一般にストリーミングと呼ばれているコンテンツ伝送方式も実現可能である。ストリーミング方式のコンテンツ伝送の場合、送信装置から受信装置のバッファにネットワークを介してＴＣＰ／ＩＰまたはＵＤＰ／ＩＰによりコンテンツデータを伝送し、受信装置のバッファからコンテンツデータを比較的一定のレートで読み出すことによって、受信装置において連続したデータを再生することができる。

また、本発明は、ＳＭＰＴＥ（ｗｗｗ．ｓｍｐｔｅ．ｏｒｇ）において規格化されたＧＸＦファイルフォーマット（ＳＭＰＴＥ　３６０Ｍ）、および、規格化が推進されているＭＸＦファイルフォーマットに準拠したファイルの暗号化伝送にも適用可能である。

（実施の形態７）

実施の形態７について説明する。

図１９は、本発明の実施の形態７によるパケット送信手段１１０１のブロック図である。

ここで、パケット送信手段１１０１は、図４を参照して説明したパケット送受信装置４０１のパケット化手段４０３およびフレーム化手段４０９に相当する。

パケット送信手段１１０１は、一般データ入力手段１１０２と、パケット化情報入力手段１１０４と、一般データパケット化手段１１０５と、バッファ手段１１０６と、有効データ抽出手段１１０７と、優先データパケット化手段１１０９と、パケット送信順序制御手段１１１３と、フレームデータ送信手段１１１４とを備える。

パケット送信手段１１０１において、優先データが優先データ入力手段１１０３から有効データ抽出手段１１０７に入力される。有効データ抽出手段１１０７は、入力された優先データから無効なデータ成分を取り除き、有効ペイロードを抽出して有効データ１１０８を優先データパケット化手段１１０９に入力する。

優先データパケット化手段１１０９は、図８を参照して説明したパケット送受信装置４０１Ｂの第２のパケット化手段７０２に相当する。

パケット送信順序制御手段１１１３は、図８を参照して説明したパケット送受信装置４０１Ｂの送信キュー制御手段６０１に相当する。

有効データ抽出手段１１０７における処理内容としてはデータのバッファリング、データビット数変換、クロック周波数変換などを含む。

具体例としては、優先データのストリームとしてＳＭＰＴＥ３２１Ｍ規格のＳＤＴＩストリームがあり、また、有効データとしてＳＭＰＴＥ３１４Ｍ規格のＤＩＦデータがある。

あるいは、優先データのストリームとしてＤＶＢ、Ａ１０Ｍ規格のＤＶＢ－ＡＳＩストリームがあり、また、有効データとしてＭＰＥＧ規格のＭＰＥＧ－ＴＳパケットがある。

優先データパケット化手段１１０９は、パケット化情報と、有効データ１１０８を用いて、優先データパケットを生成する。

図２０は、優先データパケットのプロトコルスタックを説明するための模式図である。

図２０に示したＡＶデータは、本実施の形態において、優先データ入力手段１１０３から入力される優先データである。

図２０に示したようにＡＶデータを処理することによって、イーサネット（Ｒ）フレームが生成される。

一方、一般データ入力手段１１０２は、一般データが入力される。一般データは、一般的に、必ずしもリアルタイムで送る必要の無いデータである。一般化データパケット化手段１１０５は、一般データを用いて一般データパケットを生成し、一般データパケットを出力する。なお、一般データ入力手段１１０２はデータのインタフェースを行うものである。

一般化データパケット化手段１１０５は、図８を参照して説明したパケット送

受信装置４０１Ｂの第１のパケット化手段７０１に対応する。

一般データの例としては、前述した機器の動作制御に関する情報、ＳＮＭＰおよびＭＩＢ等の管理情報があり、これらはＴＣＰ／ＩＰあるいはＵＤＰ／ＩＰを用いて伝送される。

一般データパケット化手段１１０５から出力される一般データパケットは、バッファ手段１１０６に入力され、バッファ手段１１０６は一般データパケットを一時的に蓄積する。ここで、バッファ手段１１０６に一般データパケットが蓄積されると、バッファ手段１１０６はパケット送信順序制御手段１１１３に送信要求信号１１１０を通知（アサート）して送信要求を行う。

一般的に、ビデオデータなどのコンテンツデータをリアルタイムでストリーム伝送するためには、リアルタイム性を必要としないデータよりもビデオデータを優先的に処理する必要がある。

パケット送信順序制御手段１１１３は、優先データパケットの送信を優先させつつ、送信要求信号１１１０がアサートされた場合には、優先データパケットのリアルタイム性を損なわない範囲で一般データパケット１１１２の送信を許可する。送信許可は、バッファ手段１１０６に対する送信許可信号１１１１をアサートすることにより、バッファ手段１１０６から一般データパケットを送信することを許可する。

フレームデータ送信手段１１１４は、パケット送信順序制御手段１１１３から入力された送信パケットを用いて、イーサネット（R）フレームを生成し、送信フレームとしてネットワークに出力する。

図２１は、本実施の形態における送信タイミングチャートを説明するための模式図である。このタイミングチャートに例示する方式は、本実施の形態の要点の１つである優先データパケットと非優先データパケット（一般データパケット）の送信制御方式である。

図２１では、送信パケット２１０３の送信開始タイミング２１０１と、送信要

求信号１１１０のパルス波形２１０２と、送信パケット２１０３とを時間的に対応するように示している。

送信開始タイミング２１０１では、優先データパケットを含む送信フレームが送信されるタイミングを上向き矢印で示し、非優先データパケットを含む送信フレームが送信可能なタイミングを下向き矢印で示している。

また、送信パケット２１０３は優先データパケットを白抜き、非優先データパケットを黒塗りで示している。

本実施の形態では、一例として以下のような優先データを送信する場合を例として説明する。優先データが、ＤＶＣＰＲＯ２５（ＳＭＰＴＥ３１４Ｍで規定）である場合、ＮＴＳＣモードでは１フレーム期間に１２０，０００バイトのデータが発生するので、データレートは約５７．６メガビット／秒（約５７．６Ｍｂｐｓ）の一定レート（ＣＢＲ）となる。ここでは、ＡＶデータのビデオペイロード長を１２００バイト、システムクロックは２７ＭＨｚとしている。

優先データであるＡＶデータのパケット発生率は、１２０，０００／１，２００＝１００パケット／フレーム＝２９９７パケット／秒となる。

したがって、優先データパケットのみを伝送する場合であれば、２７０００００／２９９７＝９００９．９クロックに一回パケットを送信すればよい。つまり９００９．９クロックが平均送信間隔である。

本実施の形態によれば、この平均送信間隔より短い間隔で優先データパケットを送信することにより、非優先データパケットを送信するタイミング余裕（送信余裕期間）を創り出している。

具体的には、優先データパケットの送信間隔を８１００クロックとし、優先データパケット９回毎に１回、非優先データパケットの送信を許可可能な送信余裕期間を創り出す。９００９．９クロックで９個の優先パケットを送信する場合は９００９．９＊９＝８１０８９．１クロックを要する。ここでは議論を簡単にするため、平均値で検討する。ただし、小数点以下の数値も用いている。

本実施の形態では９００９．９クロックよりも短い８１００クロックで送信するので、実際には、８１００＊９＝７２９００クロックが必要である。

したがって非優先データパケットを送信する送信余裕期間は８１０８９．１－７２９００＝８１８９．１クロックである。

送信開始タイミング２００１において、優先データパケットを送信するタイングを示す上向き矢印から次の矢印までの間隔は８１００クロックである。９回の優先パケット送信タイミングに１回、非優先パケットの送信タイミングが現れる（２１０４、２１０５，２１０６）。非優先パケットの送信タイミングを示す下向き矢印から次の矢印までの間隔は８１８９クロックである。

パルス波形２１０２に示されるように、送信要求信号１１１０はバッファ手段１１０６に、送信すべき一般データが蓄積されると、送信要求信号をアサートする。図２１においてはパルス波形２１０２がＨｉｇｈになる。

パルス波形２１０２において、送信要求信号１１１０がタイミング２１０７のいてＨｉｇｈになり、次に、送信開始タイミング２１０１において、一般データパケットの送信可能タイミングになったタイミング（タイミング２１０８）で送信許可信号１１１１がアサートされ（図２１には図示せず）、一般データパケット２１１１が送信される。一般データパケットが送信開始されたタイミングで送信要求信号１１１０はデアサートされる（パルス波形２１０２のタイミング２１０８）。

タイミング２１０５では、送信要求信号１１１０がアサートされていないので送信すべき一般データパケットはバッファ手段１０６には存在せず、タイミング２１０５において一般データパケットは送信されない。

つぎにタイミング２１０９で送信要求信号１１１０のパルス波形２１０２が再びアサートされ、タイミング２１１０で一般データパケット２１１２が送信される。送信要求信号１１１０は一般データパケット２１１２が送信開始されるとデアサートされる（パルス波形２１０２のタイミング２１１０）。

なお、バッファ手段１１０６に複数の一般データパケットが蓄積されている場合は、一つの一般データパケットが送信されても、送信要求信号１１１０はデアサートされず、残りの一般データパケットは次の一般データパケットの送信可能タイミングを待って、１パケットずつ送信される。このようにして優先データパケットが優先的に送信される。

送信パケットは、上記のようにパケット送信順序制御手段１１１３からフレームデータ送信手段１１１４に出力される。フレームデータ送信手段１１１４は、入力された送信パケットを用いて、物理層とのインタフェースが可能なイーサネット（R）フレームを生成し、送信フレームとして転送する。なお、１０Ｍｂｐｓおよび１００Ｍｂｐｓのイーサネット（R）ではＭＩＩ標準インタフェースが規定されており、ギガビットイーサネット（R）ではＧＭＩＩ標準インタフェースが規定されている。

なお、本実施の形態では、優先データパケットと一般データパケットの送信制御をクロック単位でそれぞれのパケットに割り当てる時間を決めたが、本発明は、これに限定されない。本発明は、例えば、優先データパケット化手段１１０９のバッファに一定量の優先データパケットを格納し、優先データパケットの平均パケット生成量よりも短い時間間隔でパケット送信順序制御手段１１１３で優先的に送信を行い、バッファでの優先パケットの格納量が、あるスレッシュルドレベル以下になったときに一般データパケットに送信を割り当てるなどとしてもよい。

以上のように、本実施の形態では優先データから有効データを抜き出し、優先データパケットとして一般データパケットよりも優先して送信することが可能である。

図２２は、本発明の実施の形態７の変形例によるパケット送信手段１１０１Ａを示すブロック図である。

パケット送信手段１１０１Ａは、有効データ抽出手段１１０７から、優先データのフォーマットに関する情報を示す優先データフォーマット情報を優先データ

フォーマット情報出力手段１２０１を介して外部に出力する点を除いて、図１９を参照して説明したパケット送信手段１１０１と同様の構成を有している。したがって、以下の説明では、主に、優先データフォーマット情報出力手段１２０１について説明する。

パケット送信手段１１０１Ａにおいて、出力される優先データのフォーマット情報を用いて外部のコンピュータ等で優先データのパケット化情報を設定すると、効率的にパケットの送信を行うことができる。

（実施の形態８）

実施の形態８について説明する。

図２３は、本発明の実施の形態８によるパケット送信手段１１０１Ｂのブロック図である。

パケット送信手段１１０１Ｂは、優先データパケット化情報生成ブロック１３０１を含み、有効データ抽出手段１１０７から、優先データフォーマット情報を優先データパケット化情報生成ブロック１３０１に出力する点を除いて、図１９を参照して説明したパケット送信手段１１０１と同様の構成を有している。したがって、以下の説明では、主に、優先データパケット化情報生成ブロック１３０１について説明する。

優先データパケット化情報生成ブロック１３０１にはパケット化情報が入力され、優先データパケット化情報生成ブロック１３０１は、パケット化情報と優先データフォーマット情報とを用いて、優先データのパケット化情報を更に最適に設定しなおす。これにより、外部においてパケット化情報をラフに生成した場合でも最適なパケット化情報を生成できるため、より効率的にパケットを送信することができる。

本実施の形態によれば、有効データ抽出手段１１０７から優先データフォーマット情報を得て、外部から入力されるパケット化情報と共にパケット化パラメー

タの決定に使用することができる。これにより、たとえば、優先データがＤＶ系の場合はＤＩＦブロックの８０バイト単位、また、ＭＰＥＧ系の場合はＴＳパケットの１８８バイト単位で優先データのパケット化を自動的に行うことができる。

図２４は、本発明の実施の形態８の変形例によるパケット送信手段１１０１Ｃのブロック図である。

パケット送信手段１１０１Ｃは、ＭＴＵ（Ｍａｘｉｍｕｍ　Ｔｒａｎｓｆｅｒ　Ｕｎｉｔ）サイズ入力手段１４０１を設けた点を除いて、図２３を参照して説明したパケット送信手段１１０１Ｂと同様の構成を有している。したがって、以下の説明では、主に、ＭＴＵサイズ入力手段１４０１について説明する。

パケット送信手段１１０１Ｃでは、ＭＴＵサイズ（最大伝送サイズ）がＭＴＵサイズ入力手段１４０１から入力される。ＭＴＵサイズは伝送路における優先データの最大伝送パケットサイズを意味する。優先データパケット化情報生成ブロック１３０１は、優先データパケット化手段１１０９にて生成される優先データパケットのサイズが入力されるＭＴＵサイズ以下になるするようにパケット化情報１４０２を生成する。これにより、優先データ送信におけるフラグメント化を防止でき、安定して優先データを通信することが実現できる。

（実施の形態９）

実施の形態９について説明する。

図２５は、本発明の実施の形態９による優先データパケット化手段１１０９のブロック図である。

優先データパケット化手段１１０９は、実施の形態２において図８を参照して説明された第２のパケット手段７０２に含まれている。

優先データパケット化手段１１０９は、バッファ手段１５０１と、バッファ手段１５０１と、パケットヘッダ生成手段１５０３と、パケット合成手段１５０４とを含む。

優先データパケット化手段１１０９において、有効データ１１０８がバッファ手段１５０１およびカウンタ手段１５０２に入力される。有効データ１１０８は、クロック信号とデータとデータ有効フラグとを含む。

バッファ手段１５０１は、有効データ１１０８のデータ有効フラグがアサート（有効）されている時ときのみデータを蓄積する。

また、カウンタ手段１５０２も、同様に有効データ１１０８のデータ量をカウントして内部のレジスタに保持する。

一方、パケット化情報１１０４（１３０２、１４０２）がパケットヘッダ生成手段１５０３に入力され、ここで、ＵＤＰ／ＩＰパケットヘッダが生成されパケット合成手段１５０４に入力される。また、パケットヘッダ生成手段１５０３から、パケット（例えば、ＩＰパケット）のペイロード長がカウンタ１５０２に出力され、カウンタ手段１５０２からこのペイロード長分の優先データを読み出すための制御信号がバッファ手段１５０１に送られる。

これによりバッファ手段１５０１は、パケットヘッダ生成手段１５０３により指定されたペイロード長の優先データをパケット合成手段１５０４に出力する。パケット合成手段１５０４は、パケットヘッダ生成手段１５０３にて生成されたＵＤＰ／ＩＰパケットヘッダと、指定されたペイロード長の優先データとを合成してＵＤＰ／ＩＰパケットを生成し、出力手段１５０５から出力する。

図２６は、本発明の実施の形態９の変形例による優先データパケット化手段１１０９Ａのブロック図である。

優先データパケット化手段１１０９Ａは、カウンタ手段１５０２からパケットヘッダ生成手段１５０３に優先データパケットのペイロード長を示す情報が入力される経路１６０１が設けられている点を除いて、図２５を参照して説明した優先データパケット化手段１１０９と同様の構成を有している。したがって、以下の説明では、主に、この経路１６０１について説明する。

優先データパケット化手段１１０９Ａにおいて、カウンタ手段１５０２より優

先データパケットのペイロード長を示す情報がパケットヘッダ生成手段１５０３にこの経路１６０１を介して入力される。パケットヘッダ生成合成手段１５０３は入力されたパケット化情報１１０４（１３０２、１４０２）とパケットペイロード長とを用いてパケットヘッダを決定する。

図２７は、本発明の実施の形態９の別の変形例による優先データパケット化手段１１０９Ｂのブロック図である。

優先データパケット化手段１１０９Ｂは、エラー訂正付加手段１７０１がさらに設けられている点を除いて、図２６を参照して説明した優先データパケット化手段１１０９Ａと同様の構成を有している。したがって、以下の説明では、主に、エラー訂正付加手段１７０１について説明する。

優先データパケット化手段１１０９Ｂにおいて、バッファ手段１５０１より優先データパケットのペイロードがエラー訂正付加手段１７０１に入力される。エラー訂正付加手段１７０１では後述するパリティ付加方式またはリードソロモン方式により、エラー訂正符号を付加して生成されたパケットをパケット合成手段１５０４に入力する。

なお、優先データパケットの例としては、図２０に示したように１次元で表現されたＡＶデータを用いてもよいが、ＡＶデータとして２次元的なマトリックスデータを利用することもできる。

図２８は、エラー訂正がリードソロモン方式の場合のパケット構成を示す図である。

図２８に示すように、縦方向m行（mは整数で、例えば図２８では４８行）と横方向ｎ列（ｎは整数で、例えば図２８では１２００バイト）のマトリックス上にバイト単位（８ビット単位）で配置されたＡＶデータマトリックスにリードソロモン形式のエラー訂正を行い、４行分の誤り訂正データを付加したデータマトリックスを（横１２００バイト、縦５２行）を生成し、データマトリックスの１行ずつを読み出し、シーケンス番号または信号フォーマット情報などをヘッダ情

報として付加したデータを優先データパケットとしてもよい。

図２９は、エラー訂正がパリティ処理方式の場合のパケット構成を示す図である。

ＡＶデータとしては、縦方向m行（mは整数で、例えば図２９では８行）と横方向ｎ列（ｎは整数で、例えば図２９では１２００バイト）のマトリックス上にバイト単位（８ビット単位）で配置されたＡＶデータマトリックスに縦の列方向にパリティ計算をして、１行分のパリティデータを付加したデータマトリックスを生成し、前記データマトリックスの１行ずつを読み出し、シーケンス番号や信号フォーマット情報などをヘッダ情報として付加したデータを優先データパケットとしてもよい。

さらに、優先データパケットを生成する別のマトリックス単位の例として、縦方向m行（mは整数で、例えば１５）と横方向ｎ列（ｎは整数で、例えば８０）のマトリックスをｋ個（ｋは整数で、例えば５）生成し、まずｋ個のマトリックスの同じ行にまず１行ずつデータを埋め込んでいくいわゆるｋ個のマトリックにおける行単位のデータインターリーブ処理を行ない、あるm行ｎ列のマトリックデータが埋まった時点でマトリックスに縦の列方向にパリティ計算をして、１行分のパリティデータを付加したデータマトリックスを生成し、前記ｋ個のデータマトリックスの１行目のデータをｋ個読み出し、次に前記ｋ個のデータマトリックスの２行目のデータをｋ個読み出すという順番で、前記ｋ個のデータマトリックスのm行目のデータをｋ個読み出し、これらそれぞれにシーケンス番号や信号フォーマット情報などをヘッダ情報として付加したデータを優先データパケットとしてもよい。

以上のように、送信装置内の優先データパケット化手段において、優先データにエラー訂正符号を付加することにより、ネットワークにおいてパケットロスが発生した場合にも、受信装置で優先データを復元することが可能になる。

（実施の形態１０）

実施の形態１０について説明する。

図３０は、本発明の実施の形態１０によるパケット送信手段１１０１Ｄのブロック図である。

パケット送信手段１１０１Ｄは、暗号化情報入力手段１０１１および優先データパケット化手段１１０９Ｃにおける暗号化情報入力手段１０１２を設けた点を除いて、図２３を参照して説明したパケット送信手段１１０１Ｂと同様の構成を有している。

図３１は、本発明の実施の形態１０による優先データパケット化手段１１０９Ｃのブロック図である。

優先データパケット化手段１１０９Ｃは、暗号化情報入力手段１０１２および暗号化手段１１２２が設けられた点を除いて、図２７を参照して説明した優先データパケット化手段１１０９Ｂと同様の構成を有している。

したがって、以下の説明では、主に、暗号化情報入力手段１０１１、優先データパケット化手段１１０９Ｃにおける暗号化情報入力手段１０１２および暗号化手段１１２２について説明する。

暗号化手段１１２２は、図４を参照して説明したパケット送受信装置４０１の暗号化手段４０６に相当している。

パケット送信手段１１０１Ｄにおいて、暗号化情報が暗号化情報入力手段１０１１から、優先データパケット化手段１１０９Ｃにおける暗号化情報入力手段１０１２に入力される。

優先データパケット化手段１１０９Ｃにおいて、バッファ手段１５０１から出力されたデータは、暗号化手段１１２２に入力され、暗号化情報入力手段１０１１から入力される暗号化情報を用いて暗号化される。暗号化手段１１２２で暗号化されたデータはエラー訂正付加手段１７０１に入力される。

なお、暗号化を行うために使用される情報は、送信装置の独自情報（機器ＩＤ、

機器の認証情報、マックアドレスなど）、秘密鍵、公開鍵の少なくとも１つを用いて生成した情報であり、暗号化強度の強い暗号化方式と組み合わせることにより優先データパケットに対する強固な著作権保護を提供できる。

暗号化方式に関しては、たとえば、ＤＴＣＰ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ）で使用されている暗号鍵Ｋｃを適用することができる。なお、暗号鍵Ｋｃの生成には、送信装置および受信装置でＤＴＣＰ方式に基づいた認証処理を行なえばよい。この処理は公知の技術であり、たとえば、ＤＴＬＡ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｌｉｃｅｎｃｉｎｇ　Ａｄｍｉｎｉｓｔｒａｔｏｒ）（ HYPERLINK "ｈｔｔｐ：／／ｗｗｗ．ｄｔｃｐ．ｃｏｍ／" ｈｔｔｐ：／／ｗｗｗ．ｄｔｃｐ．ｃｏｍ／、ｈｔｔｐ：／／ｗｗｗ．ｄｔｃｐ．ｃｏｍ／ｄａｔａ／ｄｔｃｐ＿ｔｕｔ．ｐｄｆ）や、書籍「ＩＥＥＥ１３９４、ＡＶ機器への応用」、高田信司監修、日刊工業新聞社、「第８章、コピープロテクション」、１３３～１４９ページにおいて説明されている。また、機器の認証情報は、公的または私的な認証機関でネットワーク等を介して適宜認証された証明情報を使用することができる。たとえば、政府認証基盤（ HYPERLINK "ｈｔｔｐ：／／ｗｗｗ．ｇｐｋｉ．ｇｏ．ｊｐ／" ｈｔｔｐ：／／ｗｗｗ．ｇｐｋｉ．ｇｏ．ｊｐ／）を参照することができる。

以上により、送信装置内の優先データのＵＤＰ／ＩＰパケット伝送に際して、優先データを暗号化した後、エラー訂正を付加することによって、ネットワークにおいてパケットロスが発生した場合にも、受信装置で優先データが復元可能になるとともに、ネットワーク上でのデータ盗聴、改竄を防止し、著作権が保護された安全性の高いＡＶデータ伝送を実現する。

（実施の形態１１）

実施の形態１１について説明する。

図３２は、本発明の実施の形態１１による優先データパケット化手段１１０９Ｄのブロック図である。

優先データパケット化手段１１０９Ｄにおいて、暗号化情報切替手段１２２１が設けられた点を除いては、図３１を参照して説明した優先データパケット化手段１１０９Ｃと同様の構成を有している。したがって、以下の説明では、主に、暗号化情報切替手段１２２１について説明する。

優先データパケット化手段１１０９Ｄにおいて、時間的に変化する暗号化情報が暗号化情報入力手段１０１２を介して暗号化切替手段１２２１に入力され、暗号化切替手段１２２１は、暗号化手段１１２２で使用される暗号化情報を切り替える。

暗号化情報の切り替えタイミングの一例としては、エラー訂正付加手段１７０１から得られる、エラー訂正マトリックス単位で切り替えるタイミングを使用することができる。これにより送信装置と受信装置との間で行う通信の暗号化強度をさらに強化しつつも、暗号の復号を着実に実現することができる。

優先データパケット化手段１１０９Ｄのバッファ手段１５０１および暗号化手段１１２２は、図８を参照して説明したパケット送受信装置４０１Ｂの暗号化手段４０６に相当する。優先データパケット化手段１１０９Ｄのカウンタ手段１５０２、パケットヘッダ生成手段１２０３および暗号化情報切替手段１２２１は、図８を参照して説明したパケット送受信装置４０１ＢのＡＫＥ手段４０２の一部および送信条件設定管理手段４０４の一部に相当する。優先データパケット化手段１１０９Ｄのパケットヘッダ生成手段１２０３およびエラー訂正付加手段１７０１は、図８を参照して説明したパケット送受信装置４０１Ｂの送信条件設定管理手段４０４、第２のパケット化手段７０２および暗号化手段４０６の一部に相当する。特に、優先データパケット化手段１１０９Ｄのエラー訂正付加手段７０１は、図１３を参照して説明した第２のパケット化手段７０２Ａのエラー訂正符号付加手段に相当している。

図３３は暗号の切り替えタイミングを説明するための模式図である。

図３３に示されるように、暗号化情報切替手段１２２１へ入力される暗号化情報は、エラー訂正マトリックスの切り替え時に切り替えられる。

暗号鍵切替に用いるタイミングとしては、エラー訂正マトリックスの終点または始点に同期して発生したタイミングである。

以上のように、エラー訂正マトリックスの位相を暗号鍵の切替位相とすることにより、暗号化強度を上げながら、暗号の復号をスムーズに実行することが可能となる。

なお、暗号鍵の切替位相としては、パケットヘッダ内に定義されたシーケンス番号の特定な値を使用してもよい。たとえば、エラー訂正が無い場合、シーケンス番号を０から６３までの整数とし、シーケンス番号が６３から０に更新されるタイミングを暗号鍵の切替位相として用いることができる。

また、暗号鍵切替手段１２２１に入力される暗号鍵を指定されたタイミングで切り替えながら暗号化手段１１２２に入力し、暗号化手段１１２２における暗号化鍵を指定の間隔で切替えてもよい。

また、ＵＤＰ／ＩＰ以外のプロトコル、たとえばＴＣＰ／ＩＰでパケットを送る場合にも、ＴＣＰヘッダ内に含まれるＴＣＰセグメントのシーケンス番号を用いることができる。なお、ＴＣＰプロトコルはＩＥＴＦ，ＲＦＣ７９３で規定されている。

（実施の形態１２）

実施の形態１２について説明する。

図３４は、本発明の実施の形態１２による優先データパケット化手段１１０９Ｅのブロック図である。

優先データパケット化手段１１０９Ｅにおいて、フォーマットとポート番号との対応テーブル１４０１が設けられた点を除いては、図３２を参照して説明した

優先データパケット化手段１１０９Ｄと同様の構成を有している。したがって、以下の説明では、主に、フォーマットとポート番号との対応テーブル１４０１について説明する。

優先データパケット化手段１１０９Ｅにおいて、パケットヘッダ生成手段１２０３は、上述した機能に加えて、さらに優先データフォーマット情報をＵＤＰポート番号と対応させる。なお、優先データフォーマット情報はパケット化情報１１０４に含まれている。

フォーマットとポート番号との対応テーブル１４０１には、優先データが使用するフォーマット情報が格納されており、入力されるパケット化情報１１０４内のフォーマット情報よりＵＤＰポート番号が決定される。パケットヘッダ生成手段１２０３は、このＵＤＰポート情報を用いてＵＤＰ／ＩＰパケットを生成する。

これにより、受信装置においてポート番号を検出するだけでフォーマット検出ができるため、受信装置での信号処理を簡単にすることが可能となる。また、２系統のストリーム処理が可能な受信装置で２つのストリームを同時受信している場合でもポート番号でフォーマットまたはチャネルの識別が可能となる。

（実施の形態１３）

実施の形態１３について説明する。

図３５は、本発明の実施の形態１３による、ＩＥＥＥ　１３９４ストリーム伝送に適用したパケット送信システム２０００のブロック図である。パケット送信システム２０００は、実施の形態１において図４を参照して説明したパケット送受信装置４０１に含まれている。

パケット送信システム２０００において、分離手段１５５２は、ＩＥＥＥ　１３９４ストリームから一般データと、優先データとを分離する。ここで、一般データは、ＡＶ／Ｃコマンドなどのアシンクロナス信号であり、また、優先データは、アイソクロナス信号である。

図３６は、本発明の実施の形態１３による、ＳＤＩ／ＳＤＴＩ／ＤＶＢ－ＡＳＩストリームの伝送に適用したパケット送信システム２５００を示すブロック図である。

パケット送信システム２５００において、ＲＳ２３２Ｃ，ＲＲＳ４２２などから入力される制御、管理用信号は一般データとして、また、ＳＤＩ／ＳＤＴＩ／ＤＶＢ－ＡＳＩストリームから分離されたデータは優先データとして使用される。

図３７は、本発明の実施の形態１３によるパケット送受信装置１１０１Ｅのブロック図である。

このパケット送受信装置１１０１Ｅには、図１９を参照して説明した実施の形態７によるパケット送信手段１１０１を適用している。

送信動作は上述の実施の形態７から１３に記載した動作と同様である。受信処理としては、受信フレームから一般データパケットと優先データパケットとを分離し、それぞれから一般データと優先データを復号し出力する。

なお、上述した実施の形態７から１３においては、パケットの順序性が保証されていない通信網で伝送する場合には、受信装置でパケットに付加されたシーケンス番号を用いて順序性の保証を行ってもよい。あるいは、後段のビデオ信号処理で順序性の保証を行ってもよい。

なお、受信側において優先パケットのフラグメント処理を行いたくない場合は、送信側において、あらかじめアプリケーションレベルの処理で、通信網においてフラグメントされない最大サイズ（ＭＴＵ）を検査し、それ以下のパケットサイズで伝送すればよい。あるいは、ＲＦＣの規格では全ての端末は５７６バイトのサイズのＩＰパケットを扱えなければならないと規定されているので、ルータ等の多くのネットワーク機器はこれ以下のＩＰパケットではフラグメントが起こらない。したがってＩＰパケットのサイズが５７６バイト以下となるように優先パケットを生成するようにすればよい。上記のように優先パケットにフラグメントが起こらない場合は、受信したパケットがフラグメントされていれば全て一般パ

ケットとして処理すればよい。なお、イーサネット（R）のＩＰパケットの最大値を越えた場合は送信端末でフラグメントしなければ行けないので、優先パケットのフラグメントを起こさせないためにはＩＰパケットの最大値以下でなければならないことは言うまでもない。

また、通信網においてフラグメントが起こる確率が非常に低い場合は、送信側で優先パケットのＩＰパケットのＩＰヘッダにフラグメント禁止のフラグを立てて伝送することにより、ルータがフラグメントせざるを得ない状態ではＩＰパケットを廃棄させることにより、受信端末のフラグメント処理負荷を軽減してもよい。この場合、非常に少数の優先パケットは損失となるが、受信側で誤り訂正あるいは誤り修整を行うことで通信品質を補償することができる。

さらに、実施の形態７から１３までは、通信網プロトコルとしてイーサネット（R）を例としたがこの限りではない。

また、ビデオ信号処理の例として、画像圧縮および伸張が行われるとしたが、圧縮されない場合でも本願発明の範囲から排除するものではない。また、あらかじめＭＰＥＧ等の方式で画像圧縮されたデータが入力される場合でも本願発明の範囲から排除するものではない。

また、ビデオではなく、オーディオ等のリアルタイムデータあるいは優先的に送受信を行うものであればどのようなものでも本発明から排除するものではない。

また、実施の形態７から１３までは、ＣＢＲ（ｃｏｎｓｔａｎｔ ｂｉｔ ｒａｔｅ）のビデオ信号を例としたが、優先データはＣＢＲに限るものではない。

また、優先パケットはハードウエア処理、一般パケットはＣＰＵ処理としたが、処理スピードが間に合うのであればこの限りではない。

なお、上記説明は、当業者が、本発明を行い、または本発明を使用できるように提供される。これらの実施形態への様々な改変は、当業者に容易に明らかであり、本明細書中に明確にされる包括的原理は、さらなる発明の使用なしに他の実施形態に適用され得る。従って、本発明は、本明細書中に示される実施形態に限

定される意図はなく、本明細書中に開示される原理および新規な特徴と一致する最も広い範囲に合致されることを意図するものである。

産業上の利用可能性

本発明によれば、パケット送受信装置は、送信データのセキュリティを確保するためのＡＫＥ手段と、送信データの暗号化手段、ＡＫＥ情報または送信制御情報を暗号化されたデータに付加するためのパケット付加情報生成手段、受信パケットからＡＫＥ情報または送信制御情報などの付加情報を抽出する手段、暗号化されたデータの復号手段と、送信パケットの送信先からフィードバックされるパケット受信状況に基づいて適切なパケット送信条件を設定する送信条件設定管理手段と、パケット化手段と、パケット受信手段と、受信条件の設定管理手段とを備える。

これにより、ＤＴＣＰ方式をインターネットの標準プロトコルであるＩＰプロトコルに実装することができる。また、ＭＰＥＧ－ＴＳなどのＡＶデータストリームを送信装置で暗号化してデータの機密性および著作権の保護などを図りながら、パケット（例えば、ＩＰパケット）をネットワークを介して伝送し、受信装置で元の信号に復号することが可能である。

本発明のある実施の形態によれば、パケット送受信手段は、送信パケットを一般パケットと優先送信されるパケットにクラス分けし、一般パケットを第１のデータキュー手段に、また、優先送信されるパケットを第２のデータキュー手段に入力する。そして、送信キュー制御手段により第１のデータキュー手段および第２のデータキュー手段に一時的に蓄積されているパケットの送信順序を制御する。

これにより、データの機密性および著作権の保護を図りながら、リアルタイム性の高いデータを優先的に伝送することができる。また、入力ストリームが２チャネル以上の複数ストリームの場合にも、それぞれのストリームに関する信号を優先データと一般データにクラス分けすることにより対応が可能である。

本発明のある実施の形態によれば、パケット化手段は、第１のパケット化手段と第２のパケット化手段とを含む。ここで、ＡＫＥ設定に関するＡＫＥ関連情報などの一般データは第１のパケット化手段に入力される。また、暗号化手段にて生成された暗号化送信データおよびＡＫＥ関連情報はハードウエアによるパケット化が実行される第２のパケット化手段に入力される。なお、ＡＫＥ関連情報とは、コピー制御情報および暗号化鍵の更新情報のことである。第１のパケット化手段の出力は第１のデータキュー手段に入力され、第２のパケット化手段の出力は第２のデータキュー手段に入力される。送信条件設定管理手段から送信キュー制御手段に対して、第２データキュー手段に一時的に蓄積されている信号を優先的に出力するためのコマンドを出すと、暗号化されたデータが優先的に出力される。

このように第２のキュー手段がオーバフローしないように制御すれば、受信装置で適切な大きさのバッファを有しているため、送信装置と受信装置との間でデータコンテンツのリアルタイム伝送が実現できる。送信装置と受信装置との間でデータを暗号化してリアルタイム伝送する際に、第２のパケット化手段がハードウエアで構成されているため、ソフトウエア処理が間に合わないために発生する送信パケットの送り残しおよび受信パケットの取りこぼしといった不具合が発生しない。また、データ量の小さい第１のパケット化手段は安価なマイコンなどでも構成できるため、低コスト化が図れる。

本発明のある実施の形態によれば、パケット送受信手段は、ＡＫＥ手段はＤＴＣＰ方式で規定されている処理手順に準拠し、暗号化鍵生成手段と、ＤＴＣＰ情報生成手段と、ＡＫＥコマンド送信処理手段と、ＡＫＥコマンド受信処理手段と、交換鍵生成手段と、暗号化鍵変更情報生成手段と、復号鍵生成手段とを備える。暗号化鍵生成手段は、暗号化鍵を生成し、生成した暗号化鍵を暗号化手段に入力し暗号化動作を設定する。また、ＡＫＥ情報生成手段は、外部から入力されるコピー制御情報、および、暗号化鍵生成手段から入力される鍵更新情報とを用いて

ＡＫＥ関連情報を生成する。ＡＫＥコマンド送信処理手段は、暗号化鍵生成手段より暗号化鍵を、外部よりＡＫＥパラメータを、さらにＡＫＥコマンド受信処理手段よりＡＫＥコマンド情報を受け取り、ＡＫＥ送信コマンドを生成して、出力する。ＡＫＥコマンド受信処理手段は、第１のパケット受信手段よりＡＫＥ設定制御情報を受け取り、ＡＫＥ送信処理手段、交換鍵生成手段、暗号化鍵変更情報生成手段にそれぞれ設定制御情報を出力する。暗号化鍵変更情報生成手段は、ＡＫＥコマンド受信処理手段と第１のパケット受信手段からの情報を用いて暗号化鍵変更情報を生成する。復号鍵生成手段は、交換鍵生成手段と暗号化鍵変更情報生成手段からの情報を用いて、復号鍵を生成し復号手段に出力する。

これにより、ＤＴＣＰ方式に準拠したＡＫＥ手段を用いて、ＭＰＥＰ－ＴＳなどのＡＶデータストリームを暗号化してリアルタイムに伝送することが可能となり、データの著作権保護を図ることができる。

本発明のある実施の形態によれば、パケット送受信手段は、暗号化手段にて生成された暗号化送信データおよびＡＫＥ関連情報（例えば、コピー制御情報や暗号化鍵の更新情報）が入力される第２のパケット化手段が、内部にエラー訂正符号付加手段を備えており、それにより、エラー訂正符号を付加される。

これにより、ＩＰネットワークでパケットロスまたはビットエラーなどが発生した場合にも受信装置でエラー訂正により送信データの復元が可能となる。また、第２のパケット化手段、および第２のパケット受信手段をハードウエアで構成することが容易となる。

また、本発明のある実施の形態によれば、ネットワークを用いたＡＶコンテンツの伝送に関して、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現する。これにより、伝送路にインターネットなど公衆網を使用した場合においても、リアルタイム伝送される優先データ（ＡＶデータ）の盗聴、漏洩を防止することができる。また、インターネット等で伝送されるＡＶデータの販売、課金が可能となり、安全性の高いＢ－Ｂ、Ｂ－Ｃのコンテンツ販売流通が

可能となる。

また、本発明のある実施形態によれば、ＡＶコンテンツをハードウエアで伝送処理する場合にも、一般データパケットは従来通りＣＰＵを用いてソフトウェア処理を行う。よって、ソフトウェアの追加により管理情報や制御情報などデータを一般データとして伝送させることができる。これらのデータ量は優先データ量に比べて非常に少ないので、マイコンなど安価なマイクロプロセッサーで実現可能となり低コストなシステムを実現することができる。なお、高負荷かつ高伝送レート優先パケットのプロトコル処理にも高価なＣＰＵや大規模メモリを必要としないので、これらの点からも低コストで高機能な装置を提供できる。

また、本発明のある実施の形態おいては、優先して送信される優先パケットと、この優先パケットよりも送信優先度が低い一般パケットとを時間軸上で多重して送信し、送信される優先パケットにおける優先データの平均送信データレートを、たとえば、専用ハードウエアを用いて平均入力レート以上の速度で送信するように制御する。ビデオ信号等のリアルタイム性を必要とするデータのプロトコル処理をＣＰＵによるソフトウエア処理に頼らずハードウェア処理を行うため、ソフトウエア処理で発生する処理が間に合わないという不具合が発生しない。これにより、全ての優先データパケットが完全に送信され、リアルタイム性の保証された高品質映像の伝送が可能となる。

また、一般データは一時的にバッファ手段に蓄積され、優先データ伝送が優先して行なわれる中で間欠的に伝送される。ここで、一般データの伝送レートが１Ｍｂｐｓ以下の場合は、安価なＣＰＵやマイコンなどのプロセッサを用いて一般データの伝送処理が可能である。

なお、ストリームとして入力される優先データは、ストリームの無効データ部が除去され、有効データのみを用いて、パケット化情報に基づいてパケットが生成される。ここで、通信プロトコルとしてＵＤＰ／ＩＰを使用すると、ヘッダとしては、アドレスとしてＩＰアドレス、また、サブアドレスとしてＵＤＰポート

番号を使用することとなる。

更に、優先パケットと一般パケットの送信タイミング（送信割合）をソフトウェアではなくハードウェアで制御するので、クロック単位で完全に制御可能である。これにより全ての優先パケットが完全に送信され、リアルタイム性の保証された高品質の伝送が可能となる。また、シェイピングもクロック単位で正確に行われるため、初段のルータでのパケット廃棄の発生確率が非常に少ない高品質な通信が可能となる。イーサネット（R）フレーム（２層）のレイヤでＩＰ（３層）、ＵＤＰ（４層）のヘッダを同時に検査し、優先パケットと一般パケットを分離し、優先パケットの処理をハードウェアで行うので、受信フレームの取りこぼしが発生せず、リアルタイム性が保証された高品質の通信が可能となる。

また、本発明のある実施の形態によれば、優先データと一般データを送信するだけでなく、有効データから優先データフォーマット情報を得て、外部から入力されるパケット化情報とともにパケット化パラメータの決定に使用する。これにより、たとえば、優先データがＤＶ系の場合はＤＩＦブロックの８０バイト単位、また、ＭＰＥＧ系の場合はＴＳパケットの１８８バイト単位で優先データのパケット化の自動化などを行なうことができ、送受信装置の構成を簡単にすることができる。

本発明のある実施の形態によれば、送信装置内の優先データパケット化手段において、優先データにエラー訂正符号を付加することにより、ネットワークにおいてパケットロスが発生した場合にも、受信装置で優先データを復元することが可能になる。

本発明のある実施の形態によれば、送信装置内の優先データパケット化手段における伝送エラー保護機能が実現できる。具体的には、優先データを暗号化した後、エラー訂正符号を付加することにより、ネットワークにおいてパケットロスが発生した場合にも、受信装置で優先データを復元することが可能になるとともに、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現す

る。これにより、伝送路としてインターネットなどの公衆網を使用した場合においても、リアルタイム伝送される優先データ（ＡＶデータ）の盗聴、漏洩を防止することができる。また、インターネット等で伝送されるＡＶデータの販売、課金が可能となり、安全性の高いＢ－Ｂ、Ｂ－Ｃのコンテンツ販売流通が可能となる。

本発明のある実施の形態によれば、暗号化を行なう暗号鍵を切り替えるにより、リアルタイム伝送される優先データ（ＡＶデータ）の盗聴、漏洩をより困難にすることができる。エラー訂正マトリックスの位相を暗号鍵の切替位相とすることにより、暗号鍵の切替をスムースに実行できる。インターネットなどの公衆網において、リアルタイムに伝送されるＡＶデータの暗号化パラメータが変化するため、コンテンツの盗聴、漏洩を強力に防止できる。

本発明のある実施の形態によれば、受信装置での信号処理を簡単にすることが可能となる。優先データのフォーマットやチャネル番号とポート番号の組み合わせを決めるテーブルを送信装置と受信装置に設けることにより、受信装置でポート番号を検出するだけでフォーマットの検出ができるため、受信装置での信号処理を簡単にすることが可能となる。また、２系統のストリーム処理が可能な受信装置で２つのストリームを同時に受信している場合でもポート番号でフォーマットまたはチャネルを識別することが可能となる。

また、本発明のある実施の形態によれば、一般パケットは従来通りＣＰＵを用いてソフトウェア処理を行うのでソフトウェアを追加するだけで、管理情報および制御情報などのデータを一般データとして伝送させることができる。これらのデータ量は優先データ量に比べて非常に少ないので、マイコンなど安価なマイクロプロセッサーで実現可能となり低コストなシステムを実現することができる。なお、高負荷かつ高伝送レート優先パケットのプロトコル処理にも高価なＣＰＵや大規模メモリを必要としないので、これらの点からも低コストで高機能な装置を提供できる。

請求の範囲

1． 送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、

暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも１つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、

受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、

前記復号鍵を用いて前記受信データを復号する復号手段と

を備える、パケット送受信装置。

2． 前記パケット化手段は、前記送信条件設定情報および前記認証・鍵交換手段に関連する認証・鍵交換関連情報の少なくとも１つを用いて、パケット付加情報を生成するパケット付加情報生成手段を含み、

前記パケット化手段は、前記暗号化送信データに前記パケット付加情報を付加することによって、前記送信パケットを生成し、

前記パケット受信手段は、前記送信パケットに含まれるパケット付加情報を抽出するパケット付加情報抽出手段を含む、請求の範囲第１項に記載のパケット送受信装置。

３．　前記送信パケットを用いて送信フレームを生成するフレーム化手段と、

受信フレームを受け取り、前記受信フレームから前記受信パケットを抽出するフレーム受信手段と

をさらに備える、請求の範囲第１項に記載のパケット送受信装置。

４．　前記パケット化手段にて生成された第１のパケットを一時的に蓄積する第１のキュー手段と、

前記パケット化手段にて生成された第２のパケットを一時的に蓄積する第２のキュー手段と、

前記送信条件設定情報に基づいて、前記第１のキュー手段に蓄積された前記第１のパケットおよび前記第２のキュー手段に蓄積された前記第２のパケットのいずれを送信するかを制御する送信キュー制御手段と、

前記第１のキュー手段から出力された第１のパケットおよび第２のキュー手段から出力された第２のパケットをフレーム化することによって送信フレームを生成するフレーム化手段と、

受信フレームから前記受信パケットを抽出するフレーム受信手段と

をさらに備える、請求の範囲第１項に記載のパケット送受信装置。

５．　前記送信キュー制御手段は、前記第１のパケットまたは前記第２のパケットの送信経路に関する情報と、前記第１のパケットまたは前記第２のパケットを

送信するのに必要な帯域幅に関する情報と、前記送信パケットの送信から到着までの遅延に関する情報と、前記第１のパケットまたは前記第２のパケットの優先度に関する情報とのうち少なくとも１つの情報を用いて、前記第１のキュー手段に蓄積された前記第１のパケットおよび前記第２のキュー手段に蓄積された前記第２のパケットのいずれを送信するかを制御する、請求の範囲第４項に記載のパケット送受信装置。

６．　前記送信キュー制御手段は、ＩＥＴＦ　ｒｆｃ２２０５、ｒｆｃ２２０８、ｒｆｃ２２０９で記載されたＲＳＶＰ方式、ＩＥＴＦ　ｒｆｃ２２１０、ｒｆｃ２２１１、２２１２，ｒｆｃ２２１５で記載されたＩｎｔｓｅｒｖ方式、ＩＥＴＦ　ｒｆｃ２４７４、ｒｆｃ２４７５、ｒｆｃ２５９７、ｒｆｃ２５９８で記載されたＤｉｆｆｓｅｒｖ方式のいずれか１つの制御方式を使用する、請求の範囲第５項に記載のパケット送受信装置。

７．　前記送信キュー制御手段は、前記第１のキュー手段に蓄積された前記第１のパケットおよび前記第２のキュー手段に蓄積された前記第２のパケットのうちのいずれかを選択して、選択したパケットを優先的に出力するように前記第１のキュー手段および前記第２のキュー手段を制御する、請求の範囲第４項に記載のパケット送受信装置。

８．　前記送信キュー制御手段は、前記第２のキュー手段に蓄積された前記第１のパケットの量が所定の量を超えない場合には、前記第１のキュー手段に蓄積された前記第１のパケットを優先して出力し、前記第２のキュー手段に蓄積された前記第２のパケットの量が所定の量を超える場合には、前記第２のキュー手段に蓄積された前記第２のパケットを優先的に出力するように前記第１のキュー手段および前記第２のキュー手段を制御する、請求の範囲第４項に記載のパケット送

受信装置。

９．　前記送信キュー制御手段は、前記第１のキュー手段から送信される前記第１のパケットと前記第２のキュー手段から送信される前記第２のパケットとの間隔を平均化するように前記第１のキュー手段および前記第２のキュー手段を制御する、請求の範囲第４項に記載のパケット送受信装置。

１０．　前記送信条件設定管理手段および前記受信条件設定管理手段は、前記送信フレームの送信から到着するまでの間において前記送信パケットの送信先から受信先までの経路における最大伝送パケットサイズの検出を行ない、前記最大伝送パケットサイズ情報を用いて、前記送信条件設定情報および前記受信条件設定情報を生成する、請求の範囲第１項に記載のパケット送受信装置。

１１．　前記フレーム化手段は、前記パケット化手段にて生成された前記送信パケットに、ＩＥＥＥ　８０２．３規格のフレームヘッダを付加する、請求の範囲第３項に記載のパケット送受信装置。

１２．　前記フレーム化手段は、前記パケット化手段にて生成された前記送信パケットに、ＩＥＥＥ　８０２．１Ｑ規格のフレームヘッダを付加する、請求の範囲第３項に記載のパケット送受信装置。

１３．　前記パケット化手段は、前記暗号化送信データを所定の大きさに変換し、ＩＥＴＦでＩＰｖ４またはＩＰｖ６として規定されているＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ヘッダを付加する、請求の範囲第１項に記載のパケット送受信装置。

１４．　前記パケット化手段は、ＩＰｖ４ヘッダのサービスタイプフィールド、または、サービスタイプフィールド内のＴＯＳ（Ｔｙｐｅ　ｏｆ　Ｓｅｒｖｉｃｅ）フィールドに優先パケットであることを示す情報を付加する、請求の範囲第１項に記載のパケット送受信装置。

１５．　前記パケット化手段は、ＩＰｖ６ヘッダのプライオリティフィールドに優先パケットであることを示す情報を付加する、請求の範囲第１項に記載のパケット送受信装置。

１６．　前記パケット化手段は、第１のパケット化手段と、第２のパケット化手段とを含み、

前記第１のパケット化手段は、前記送信条件設定情報および前記認証・鍵交換関連情報の少なくとも一つの情報を用いて前記第１のパケットを生成し、

前記第２のパケット化手段は、前記送信条件設定情報と、前記認証・鍵交換関連情報と、前記暗号化送信データとの少なくとも一つの情報を用いて前記第２のパケットを生成する、請求の範囲第４項に記載のパケット送受信装置。

１７．　前記パケット化手段は、前記暗号化送信データを所定の大きさに変換し、ＩＥＴＦでＩＰｖ４またはＩＰｖ６として規定されているＩＰヘッダを付加し、

前記第１のパケット化手段はソフトウエアによって構成され、前記第２のパケット化手段はハードウエアによって構成される、請求の範囲第１６項に記載のパケット送受信装置。

１８．　前記送信データを優先データと一般データとに分離するデータ分離手段をさらに備え、

前記暗号化手段は、前記優先データを暗号化し、

前記第１のパケット化手段は、前記一般データを用いて第１のパケットを生成する、請求の範囲第１６項に記載のパケット送受信装置。

１９．　前記第１のパケット化手段は、ＩＥＴＦ文書で規定されているデータ処理プロトコルであるＲＴＣＰ，ＲＴＳＰ，ＨＴＴＰ、ＴＣＰ、ＵＤＰ、ＩＰのうちの少なくとも１つのヘッダを付加する、請求の範囲第１８項に記載のパケット送受信装置。

２０．　前記第２のパケット化手段は、データにシーケンス番号を付加するか、または、ＩＥＴＦ文書で規定されているデータ処理プロトコルであるＲＴＰ，ＵＤＰ、ＨＴＴＰ、ＴＣＰ、ＩＰのうちの少なくとも１つのヘッダを付加する、請求の範囲第１８項に記載のパケット送受信装置。

２１．　前記優先データは、ＳＭＰＴＥ　２５９Ｍ規格で規定された非圧縮ＳＤ方式信号、または、ＳＭＰＴＥ　２９２Ｍ規格で規定された非圧縮ＨＤ形式、または、ＩＥＣ　６１８８３規格で規定されたＩＥＥＥ１３９４によるＤＶまたはＭＰＥＧ－ＴＳの伝送ストリーム形式、または、ＤＶＢ規格Ａ０１０で規定されたＤＶＢ－ＡＳＩによるＭＰＥＧ－ＴＳ形式、ＭＰＥＧ－ＰＳ形式、ＭＰＥＧ－ＥＳ形式、ＭＰＥＧ－ＰＥＳ形式の内の少なくとも一つのデータストリーム形式である、請求の範囲第１８項に記載のパケット送受信装置。

２２．　前記第２のパケット化手段は、エラー訂正符号付加手段を含む、請求の範囲第１６項に記載のパケット送受信装置。

２３．　前記エラー訂正符号付加手段で用いられるエラー訂正符号の方式は、リードソロモン方式、あるいはパリティ方式である、請求の範囲第２２項に記載の

パケット送受信装置。

２４．　前記暗号化鍵を示す情報は、前記フレーム化手段において前記暗号化鍵で暗号化された送信パケットを出力するより前に、前記暗号化鍵の復号情報を前記フレーム化手段から出力する、請求の範囲第１６項に記載のパケット送受信装置。

２５．　前記暗号化鍵を示す情報は、前記暗号化鍵を用いて生成された前記暗号化送信データを含む送信パケットが送信されるときよりも、前記送信フレームの送信から前記送信フレームに対応する受信フレームの受信までの時間より前に送信される、請求の範囲第２４項に記載のパケット送受信装置。

２６．　前記認証・鍵交換手段は、前記パケット送受信装置の位置情報と、前記送信パケットの到着先の位置情報または前記受信パケットの送信元の位置情報とが、あらかじめ決められた条件に合致する時に、認証を許可する、請求の範囲第１項に記載のパケット送受信装置。

２７．前記送受信管理情報は、前記パケット送受信装置の位置情報と、前記送信パケットの到着先の位置情報または前記受信パケットの送信元の位置情報との少なくとも一方を含んでいる、請求の範囲第２６項に記載のパケット送受信装置。

２８．前記位置情報は、地域コード、住所、郵便番号、または、経度・緯度により範囲が指定された情報である、請求の範囲第２７項に記載のパケット送受信装置。

２９．　前記認証・鍵交換手段は、前記パケット送受信装置と、前記送信パケッ

トの到着先または前記受信パケットの送信元との間で、前記パケット送受信装置から前記送信パケットの到着先または前記受信パケットの受信元までの片道または往復の伝播時間があらかじめ決められた制限時間より短い時間である場合に、認証を許可する、請求の範囲第２６項に記載のパケット送受信装置。

３０．　前記認証・鍵交換手段は、前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元との間の送受信区間において無線伝送区間が存在する場合、前記無線伝送区間ではデータをスクランブルして伝送するモードであることを確認した場合に、認証を許可する、請求の範囲第２６項に記載のパケット送受信装置。

３１．　前記認証・鍵交換手段は、

前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元との間で認証を行った場合に、前記送信パケットの到着先または前記受信パケットの送信元に関する情報を一時的に記憶する記憶手段と、

前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元とが前記あらかじめ決められた条件に合致しないために前記認証が成立しない場合に、前記記憶手段にて記憶された情報と、前記送信パケットの前記到着先に関する情報または前記受信パケットの前記送信先に関する情報とを照合し、前記パケット送受信装置と前記送信パケットの到着先または前記受信パケットの送信元との間で認証を行う、照合手段と

を含む、請求の範囲第２６項に記載のパケット送受信装置。

３２．　前記送信パケットの前記到着先に関する情報または前記受信パケットの前記送信先に関する情報は、証明書、ＭＡＣアドレスおよび生体情報の少なくとも１つを含む、請求の範囲第３１項に記載のパケット送受信装置。

３３．　前記認証・鍵交換手段は、予め規定された認証および鍵交換を行い、所定の期間で暗号化鍵または復号鍵を更新する、請求の範囲第１項に記載のパケット送受信装置。

３４．　前記認証・鍵交換手段が前記復号鍵を更新するタイミングを示すタイミング情報が、前記送信パケットに付加される、請求の範囲第３３項に記載のパケット送受信装置。

３５．　前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットのＴＣＰポート番号、またはＵＤＰポート番号を変化させることによって通知される、請求の範囲第３３項に記載のパケット送受信装置。

３６．　前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＨＴＴＰを使用している場合、ＨＴＴＰリクエスト毎に更新される、請求の範囲第３３項に記載のパケット送受信装置。

３７．　前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＨＴＴＰを使用している場合、一定のデータ量毎に変化される、請求の範囲第３３項に記載のパケット送受信装置。

３８．　前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＲＴＰを使用している場合、予め決められた期間内に更新される、請求の範囲第３３項に記載のパケット送受信装置。

３９．　前記認証・鍵交換手段におけるＤＴＣＰ方式のコピー制御情報は、前記

送信パケットに暗号化モード情報を付加することによって伝送される、請求の範囲第第３３項に記載のパケット送受信装置。

４０．　前記優先データのデータレートが所定の値より小さくならないように、前記送信キュー制御手段は前記第１のキュー手段および前記第２のキュー手段を制御する、請求の範囲第１８項に記載のパケット送受信装置。

４１．　前記送信キュー制御手段は、前記優先データが前記第２のキュー手段に蓄積される時間があらかじめ決めた値より常に小さくなるように、前記送信キュー制御手段は前記第１のキュー手段および前記第２のキュー手段を制御する、請求の範囲第４０項に記載のパケット送受信装置。

４２．　前記第２のパケット化手段は、データを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、前記第２のパケットのパケットヘッダを生成するパケットヘッダ生成手段と、前記パケットヘッダと前記バッファから出力されるペイロードとを組み合わせてパケットを合成するパケット合成手段とを含み、

前記パケットヘッダ生成手段は前記第２のパケットのペイロード長を指定して、前記バッファ手段に蓄積されたデータを読み出して、前記パケット合成手段に入力する、請求の範囲第４０項に記載のパケット送受信装置。

４３．　前記第２のパケット化手段は、前記優先データから抽出したデータを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、パケット化情報を用いてパケットヘッダを生成するパケットヘッダ生成手段と、前記パケットヘッダとペイロードとを組み合わせてパケットを生成するパケット生成手段とを含み、

前記カウンタ手段は前記バッファ手段からペイロード長に相当するデータを読み出すための制御データを出力する、請求の範囲第４０項に記載のパケット送受信装置。

４４．　前記第２のパケット化手段は、データを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、パケット化情報を用いてパケットヘッダを生成するパケットヘッダ生成手段と、前記データにエラー訂正を付加するエラー訂正付加手段手段と、前記パケットヘッダと前記エラー訂正を付加したデータとを合成するパケット合成手段とを含み、

前記カウンタ手段は前記バッファ手段よりペイロード長に相当するデータを読み出すための制御データを出力する、請求の範囲第４０項に記載のパケット送受信装置。

４５．　前記優先データおよび前記一般データが処理されるレイヤよりも下位レイヤの受信フレームを処理するレイヤにおいて、前記受信フレームに含まれる受信パケットの通信プロトコルヘッダから前記優先データと前記一般データを選別して、前記優先データの処理と前記一般データの処理を独立に行う、請求の範囲第４０項に記載のパケット送受信装置。

４６．　前記第２のパケット化手段は、暗号鍵切替手段を含み、前記暗号鍵切替手段に入力される暗号鍵を指定されたタイミングで切り替えながら前記暗号化手段に入力し、前記暗号化手段における暗号化鍵を指定の間隔で切替る、請求の範囲第１項に記載のパケット送受信装置。

４７．　前記暗号鍵切替に用いるタイミングとしては、前記パケットヘッダ生成手段の出力であるパケットヘッダ内の所定のシーケンス番号に同期して発生した

タイミングである、請求の範囲第４６項に記載のパケット送受信装置。

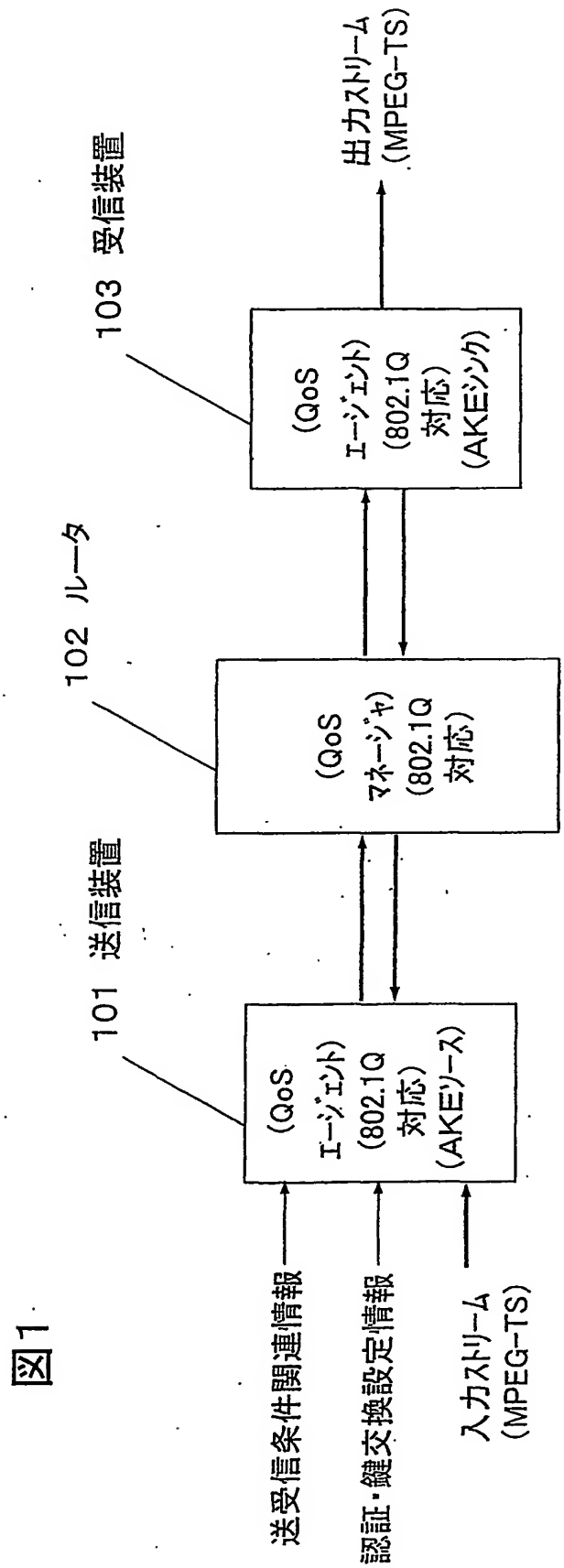
４８．　前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＨＴＴＰを使用している場合、ＨＴＴＰリクエスト毎に更新される、請求の範囲第４６項に記載のパケット送受信装置。

４９．　前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＨＴＴＰを使用している場合、一定のデータ量毎に変化される、請求の範囲第４６項に記載のパケット送受信装置。

５０．　前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがＲＴＰを使用している場合、予め決められた期間内に更新される、請求の範囲第４６項に記載のパケット送受信装置。

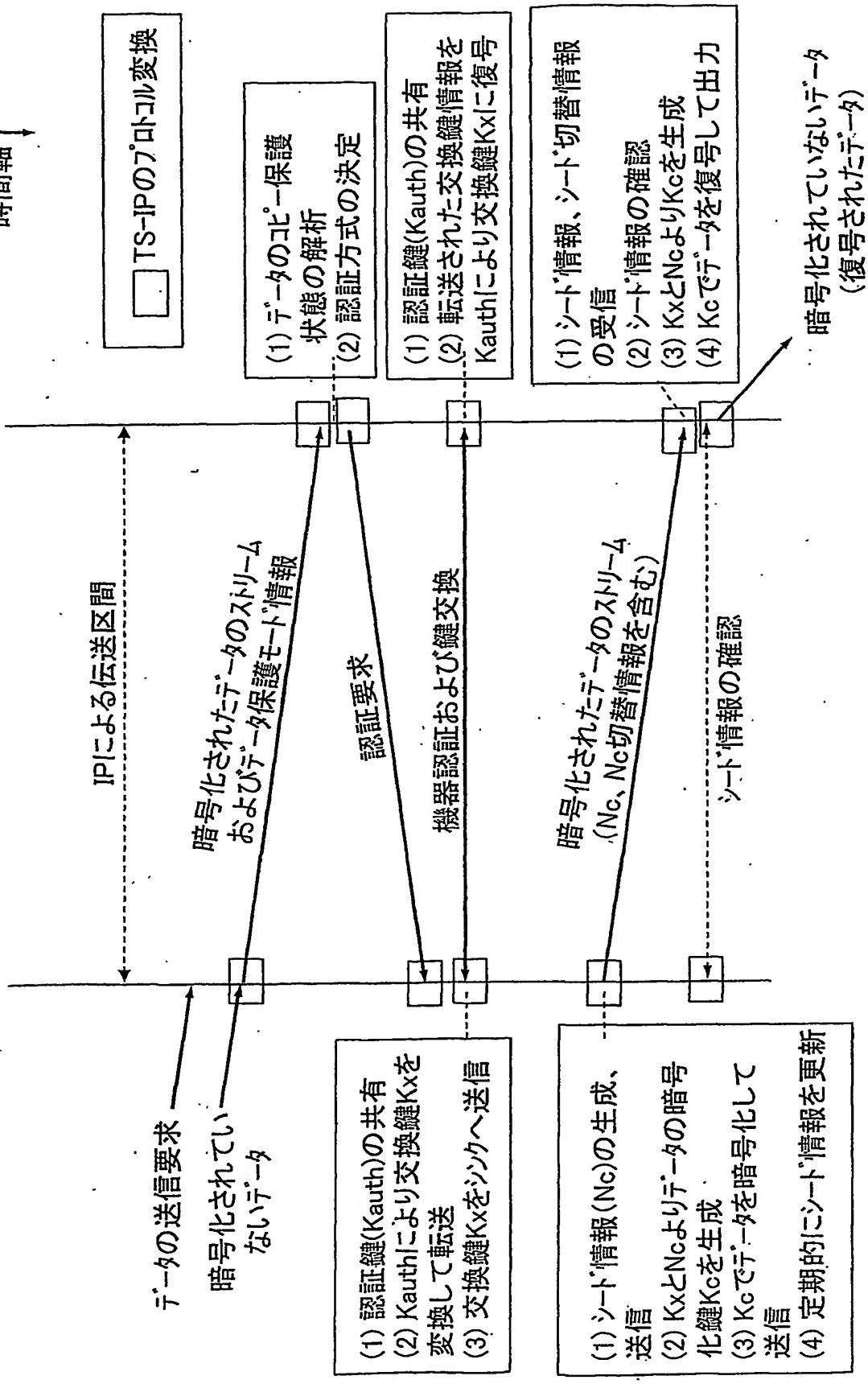
５１．　前記暗号鍵切替に用いるタイミングとしては、エラー訂正マトリックスの終点または始点に同期して発生したタイミングである、請求の範囲第４６項に記載のパケット送受信装置。

図1



差替え用紙（規則26）

図2



差替え用紙（規則26）

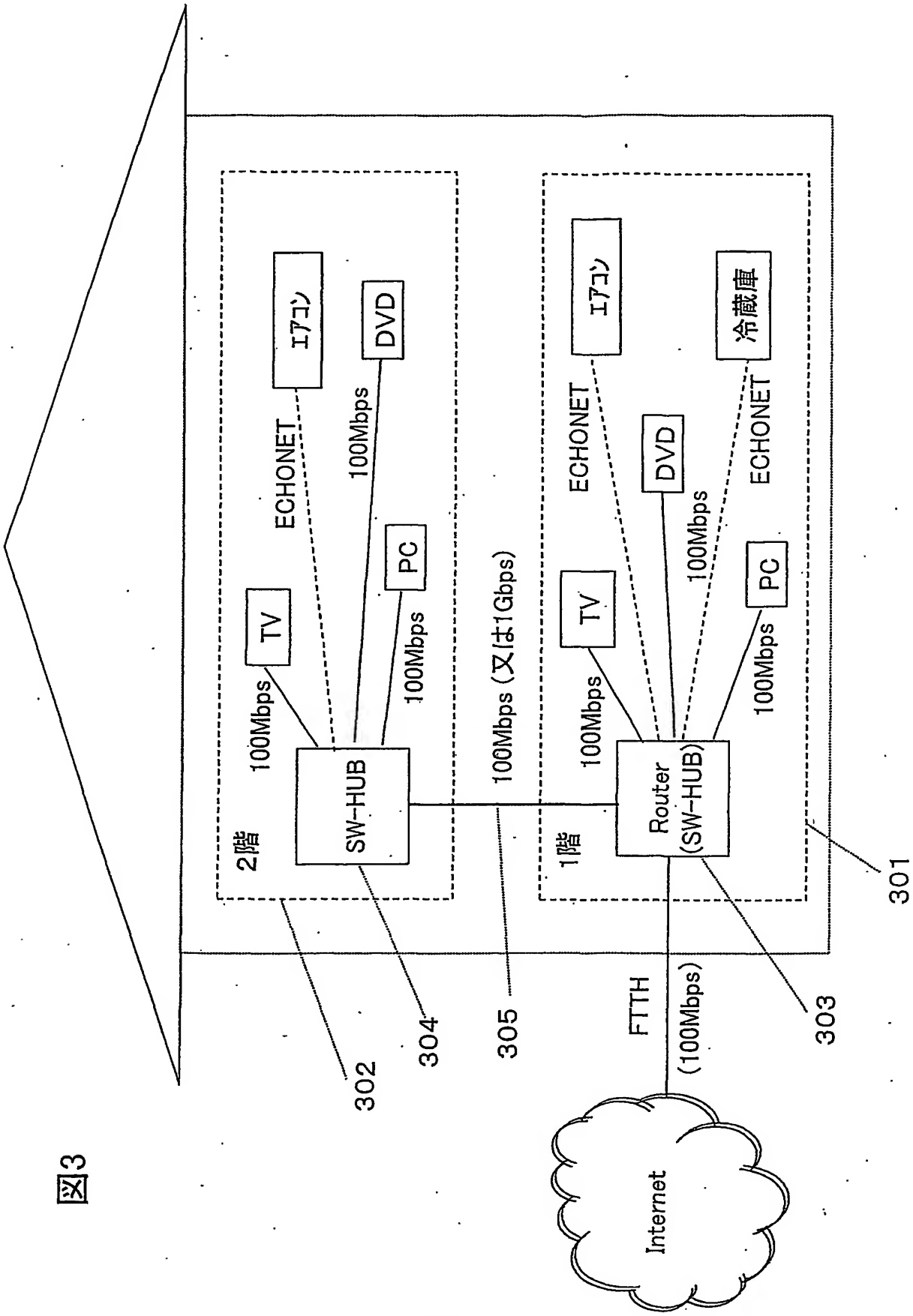


図3

差替え用紙（規則26）

図4

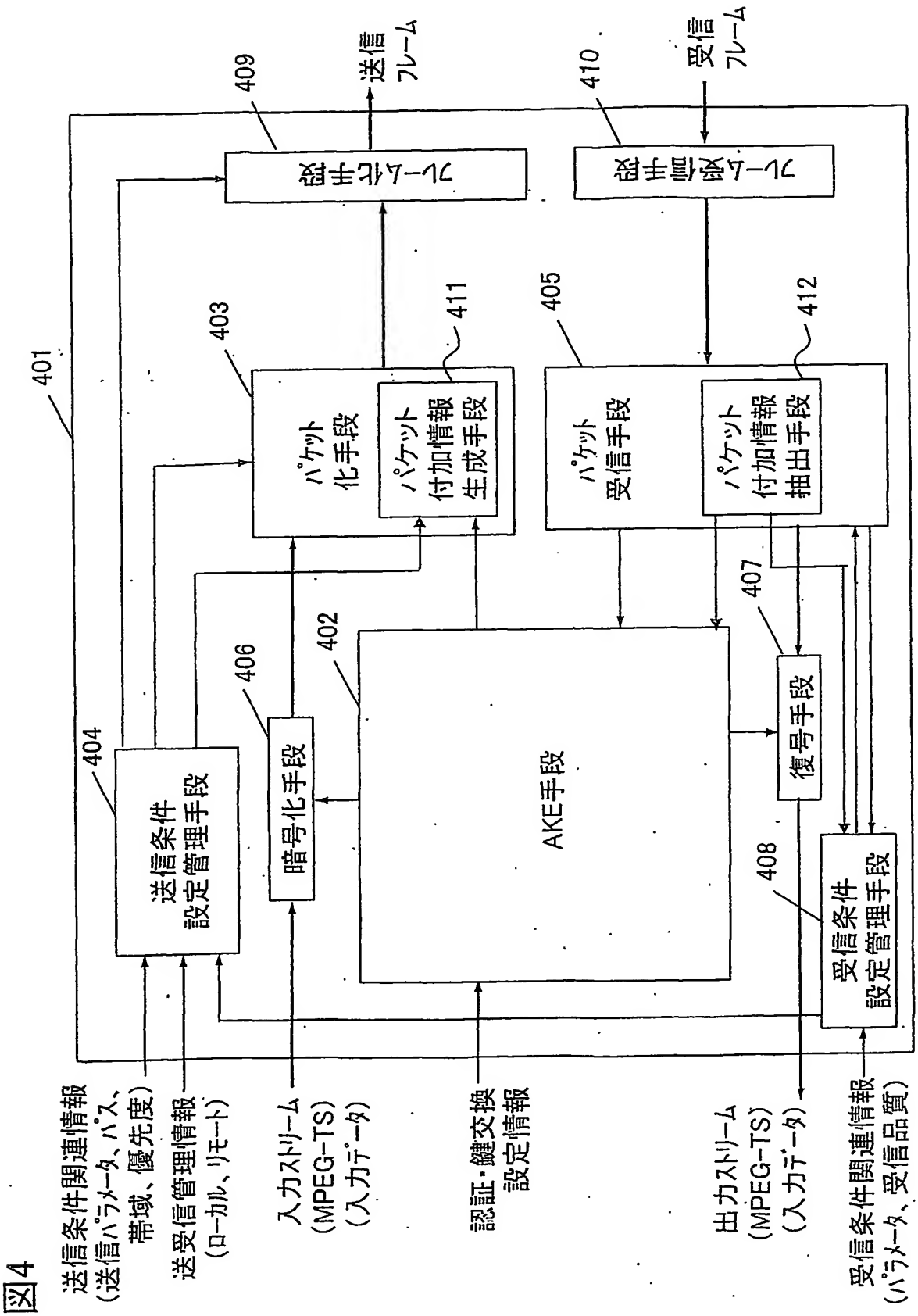

401
402
403
404
405
406
407
408
409
410
411
412
送信フレーム
受信フレーム
ネットワーク送信手段
ネットワーク受信手段
パケット化手段
パケット付加情報生成手段
パケット受信手段
パケット付加情報抽出手段
送信条件設定管理手段
暗号化手段
AKE手段
復号手段
受信条件設定管理手段
送信条件関連情報（送信パラメータ、パス、帯域、優先度）
送受信管理情報（ローカル、リモート）
入力ストリーム（MPEG-TS）（入力データ）
認証・鍵交換設定情報
出力ストリーム（MPEG-TS）（入力データ）
受信条件関連情報（パラメータ、受信品質）

図5

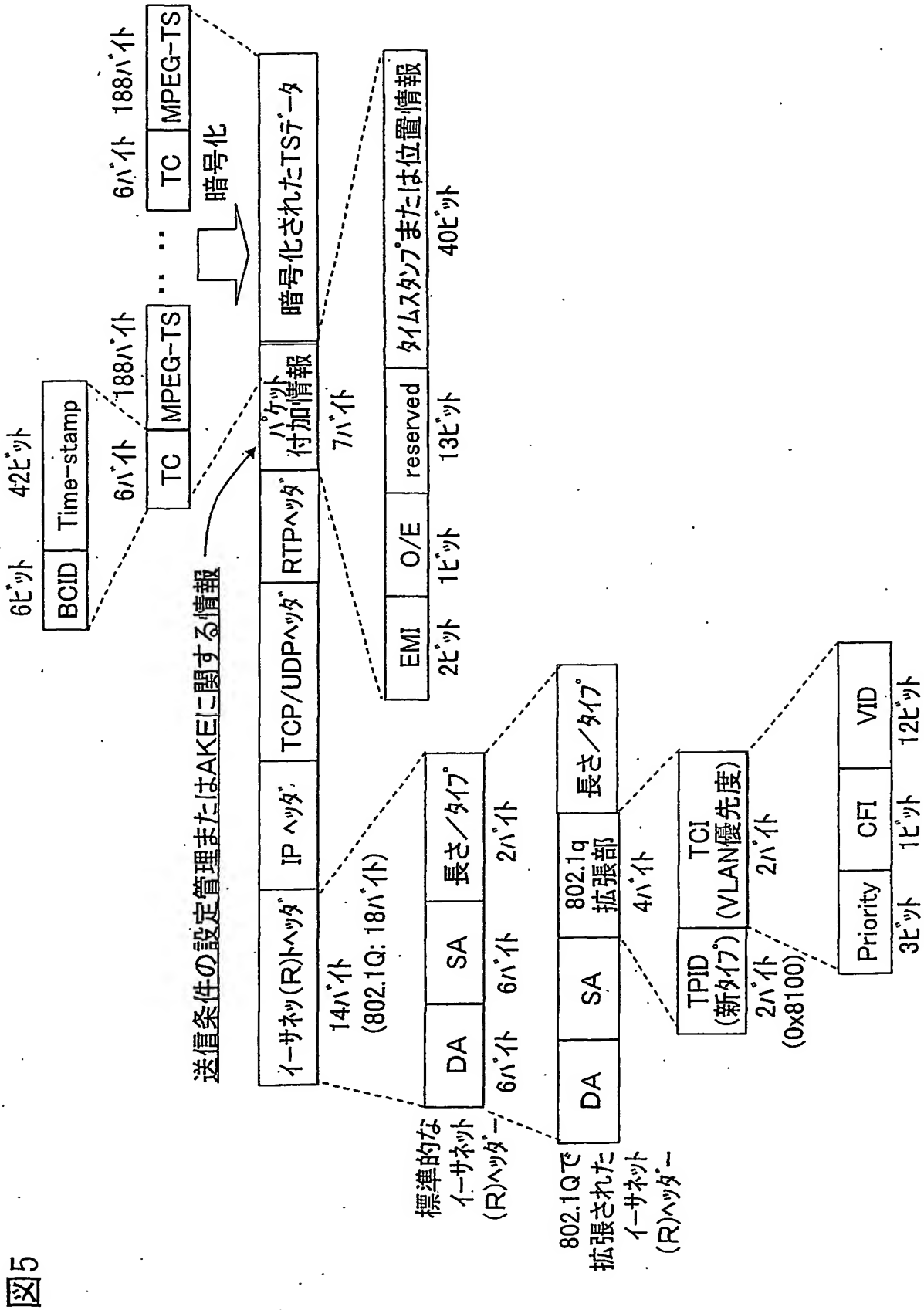
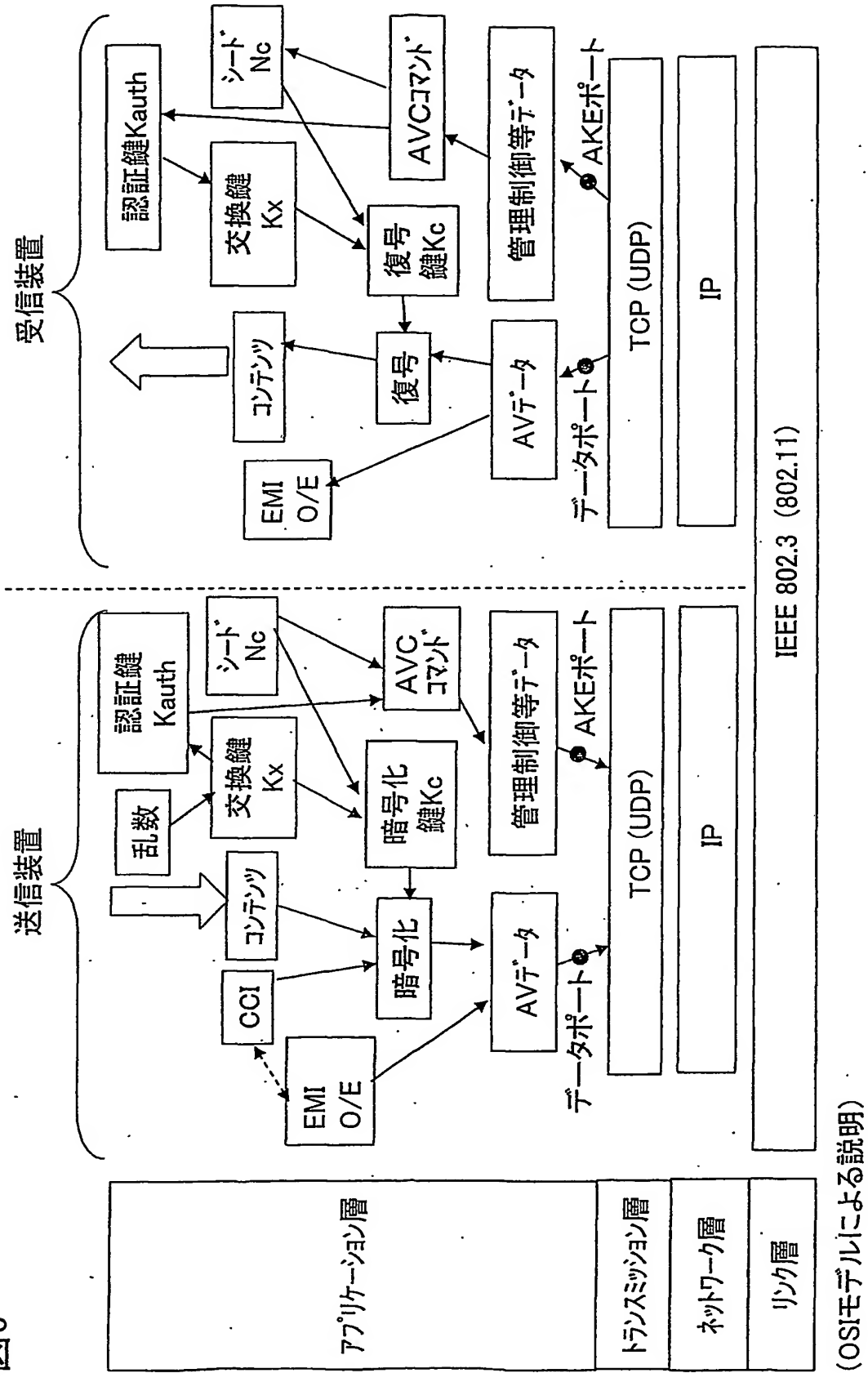
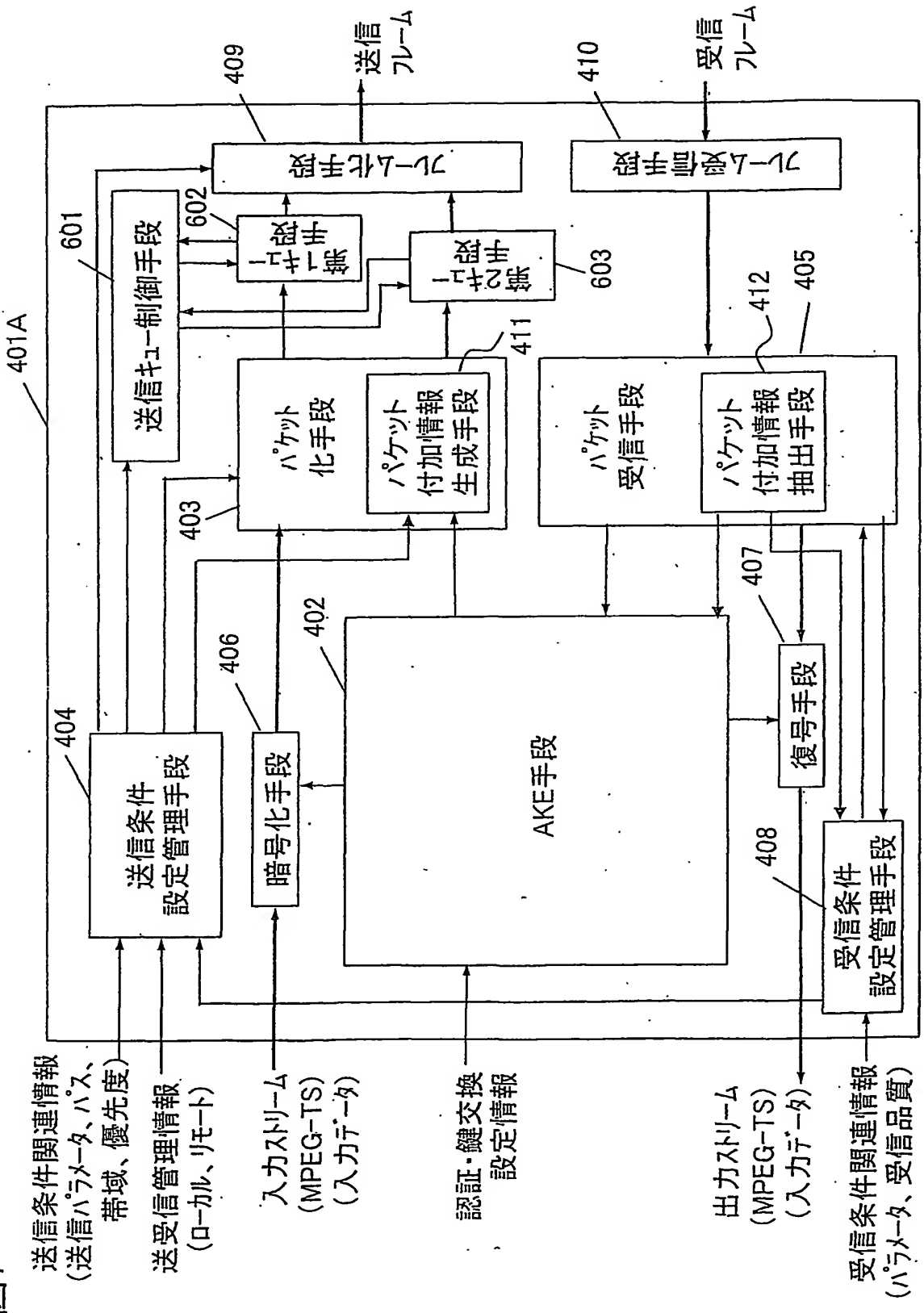

6ビット
42ビット
BCID
Time-stamp
送信条件の設定管理またはAKEに関する情報
6バイト
188バイト
TC
MPEG-TS
暗号化
6バイト
188バイト
TC
MPEG-TS
パケット付加情報
7バイト
暗号化されたTSデータ
EMI
2ビット
O/E
1ビット
reserved
13ビット
タイムスタンプまたは位置情報
40ビット
イーサネット(R)ヘッダ
IP ヘッダ
TCP/UDPヘッダ
RTPヘッダ
14バイト
(802.1Q: 18バイト)
標準的なイーサネット(R)ヘッダー
DA
SA
長さ／タイプ
6バイト
6バイト
2バイト
802.1Qで拡張されたイーサネット(R)ヘッダー
DA
SA
802.1q拡張部
長さ／タイプ
4バイト
TPID
(新タイプ)
2バイト
(0x8100)
TCI
(VLAN優先度)
2バイト
Priority
3ビット
CFI
1ビット
VID
12ビット

図6



差替え用紙（規則26）

図7


401A
409
送信フレーム
410
受信フレーム
フレーム化手段
フレーム受信手段
601
送信キュー制御手段
602
第1キュー手段
第2キュー手段
603
411
412
405
403
パケット化手段
パケット付加情報生成手段
パケット受信手段
パケット付加情報抽出手段
407
402
406
404
AKE手段
復号手段
暗号化手段
408
送信条件設定管理手段
受信条件設定管理手段
送信条件関連情報
(送信パラメータ、パス、帯域、優先度)
送受信管理情報
(ローカル、リモート)
入力ストリーム
(MPEG-TS)
(入力データ)
認証・鍵交換設定情報
出力ストリーム
(MPEG-TS)
(入力データ)
受信条件関連情報
(パラメータ、受信品質)

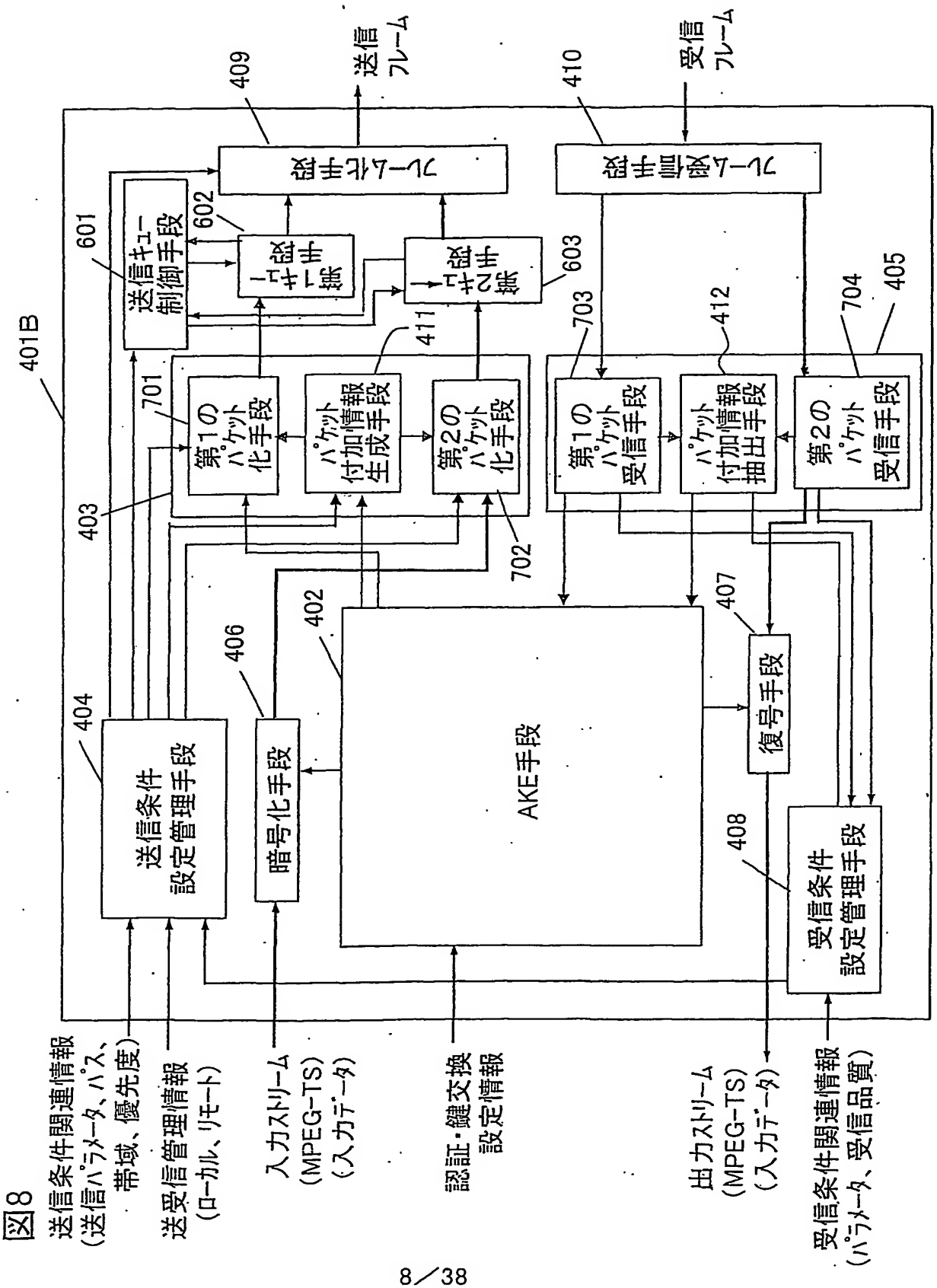
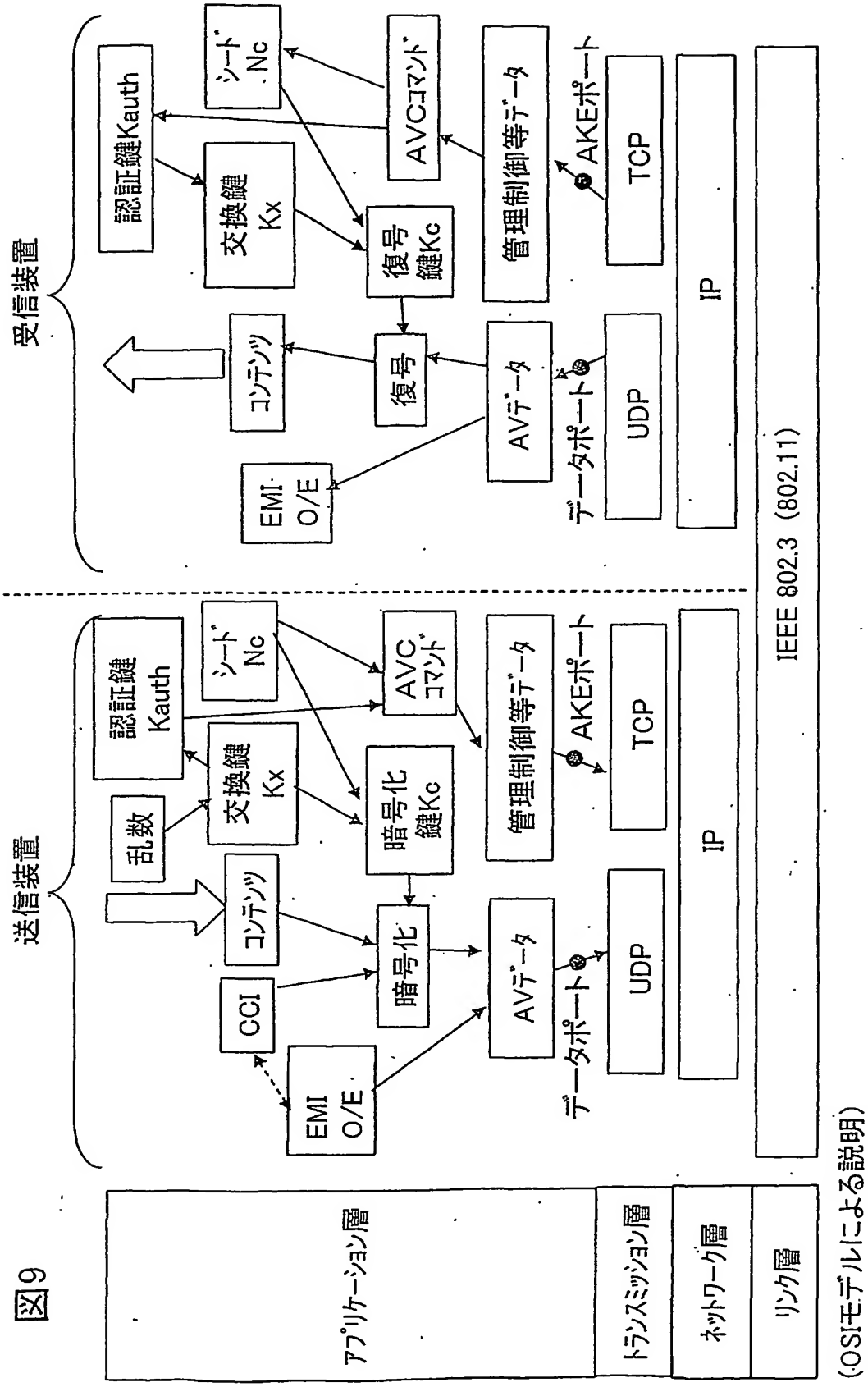

401B
送信条件関連情報
(送信パラメータ、パス、
帯域、優先度)
送受信管理情報
(ローカル、リモート)
入力ストリーム
(MPEG-TS)
(入力データ)
認証・鍵交換
設定情報
出力ストリーム
(MPEG-TS)
(入力データ)
受信条件関連情報
(パラメータ、受信品質)
送信条件
設定管理手段
暗号化手段
AKE手段
復号手段
受信条件
設定管理手段
第1の
パケット
化手段
パケット
付加情報
生成手段
第2の
パケット
化手段
第1の
パケット
受信手段
パケット
付加情報
抽出手段
第2の
パケット
受信手段
送信キュー
制御手段
送信
フレーム
受信
フレーム
403
404
405
406
407
408
409
410
411
412
601
602
603
701
702
703
704

図8

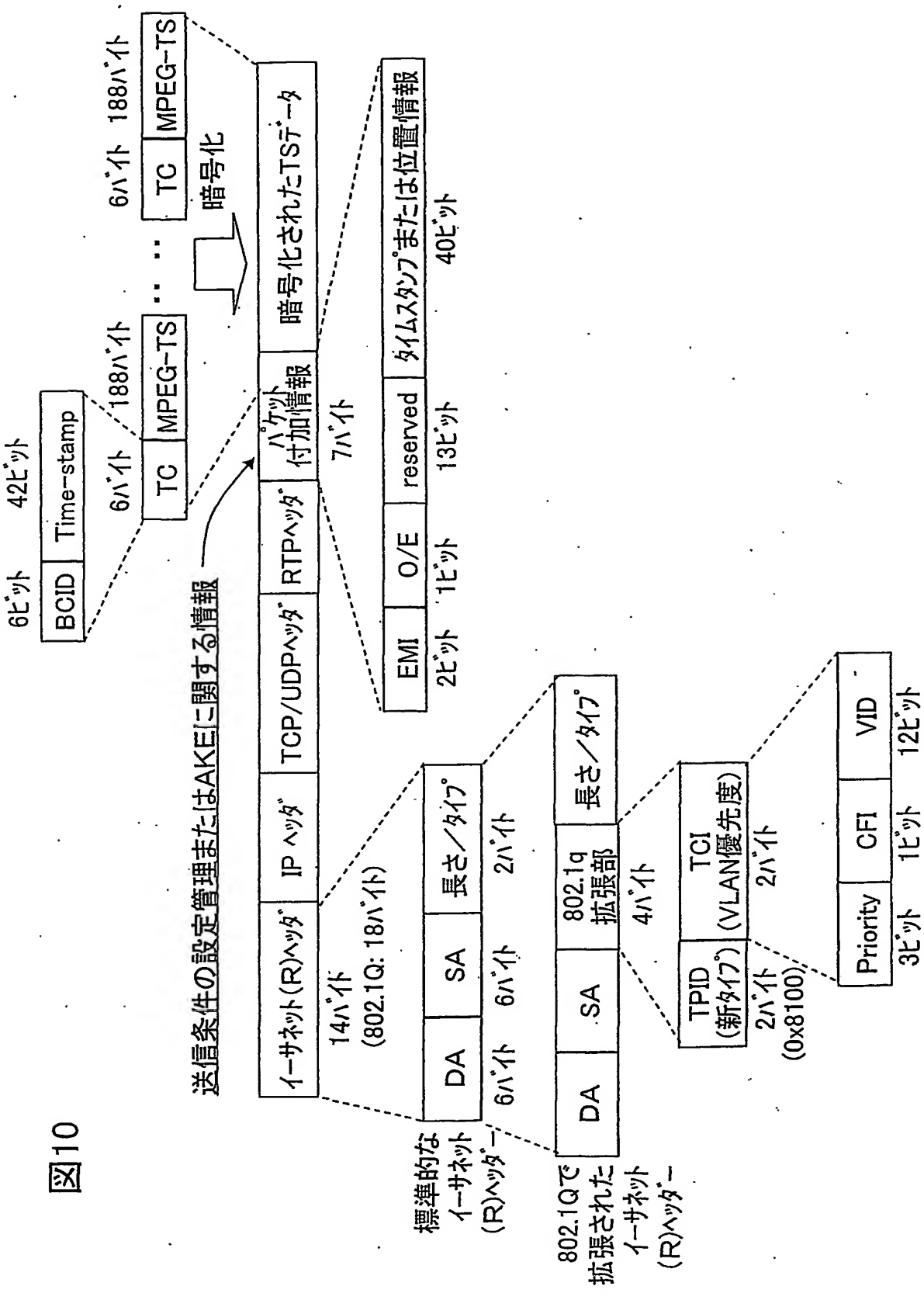
図9



(OSIモデルによる説明)

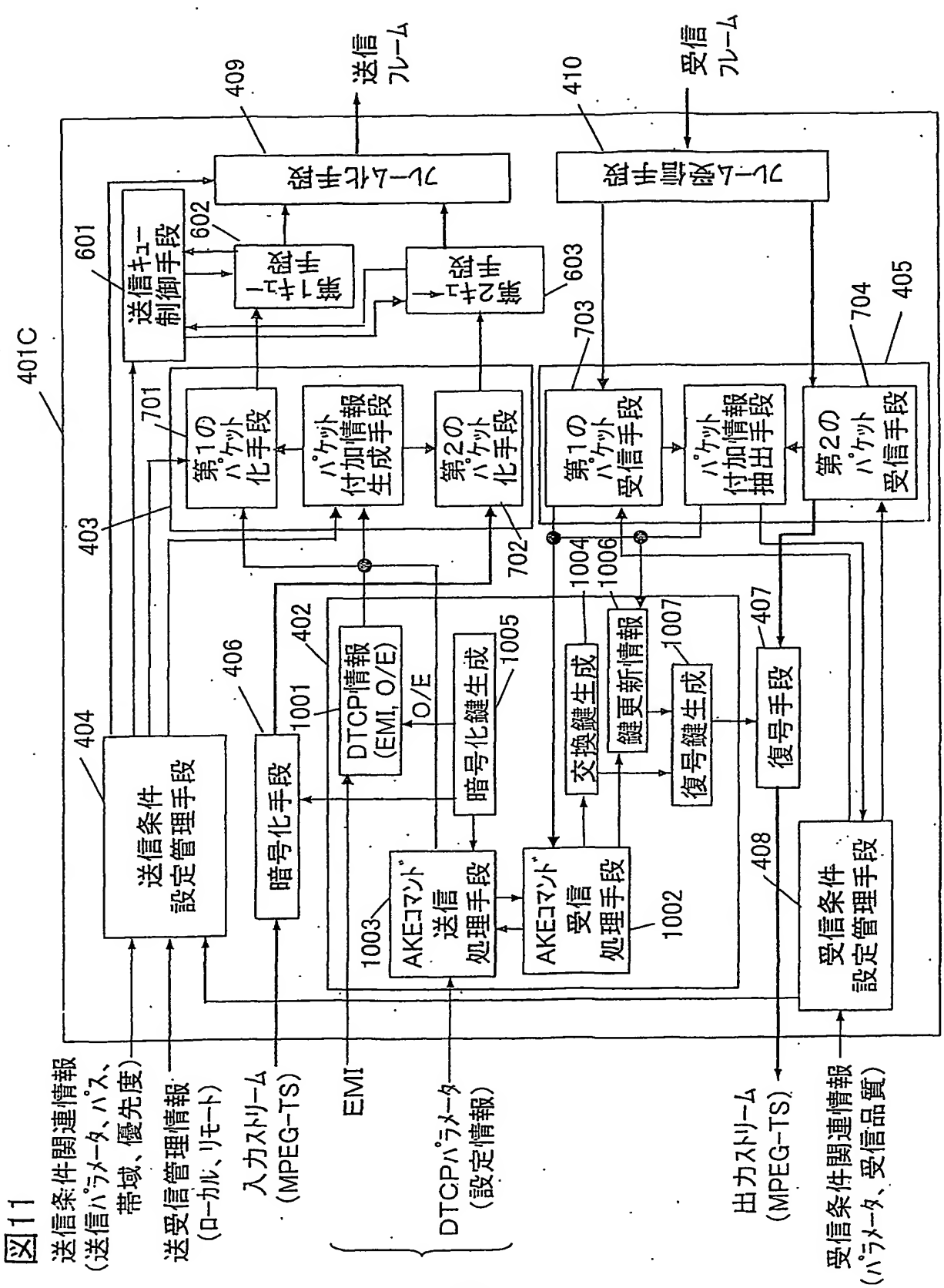
差替え用紙（規則26）

図10



差替え用紙（規則26）

図11



差替え用紙（規則26）

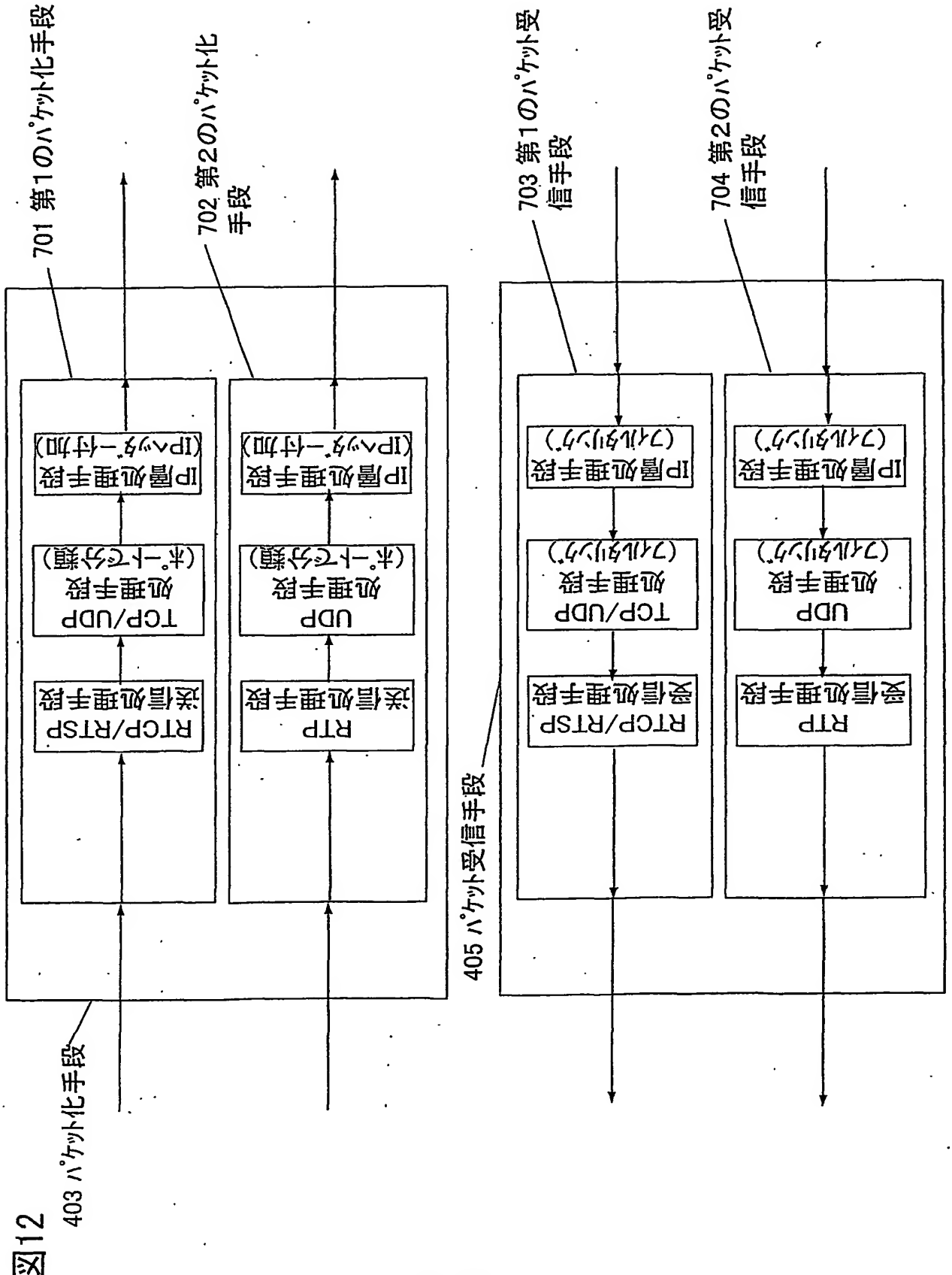
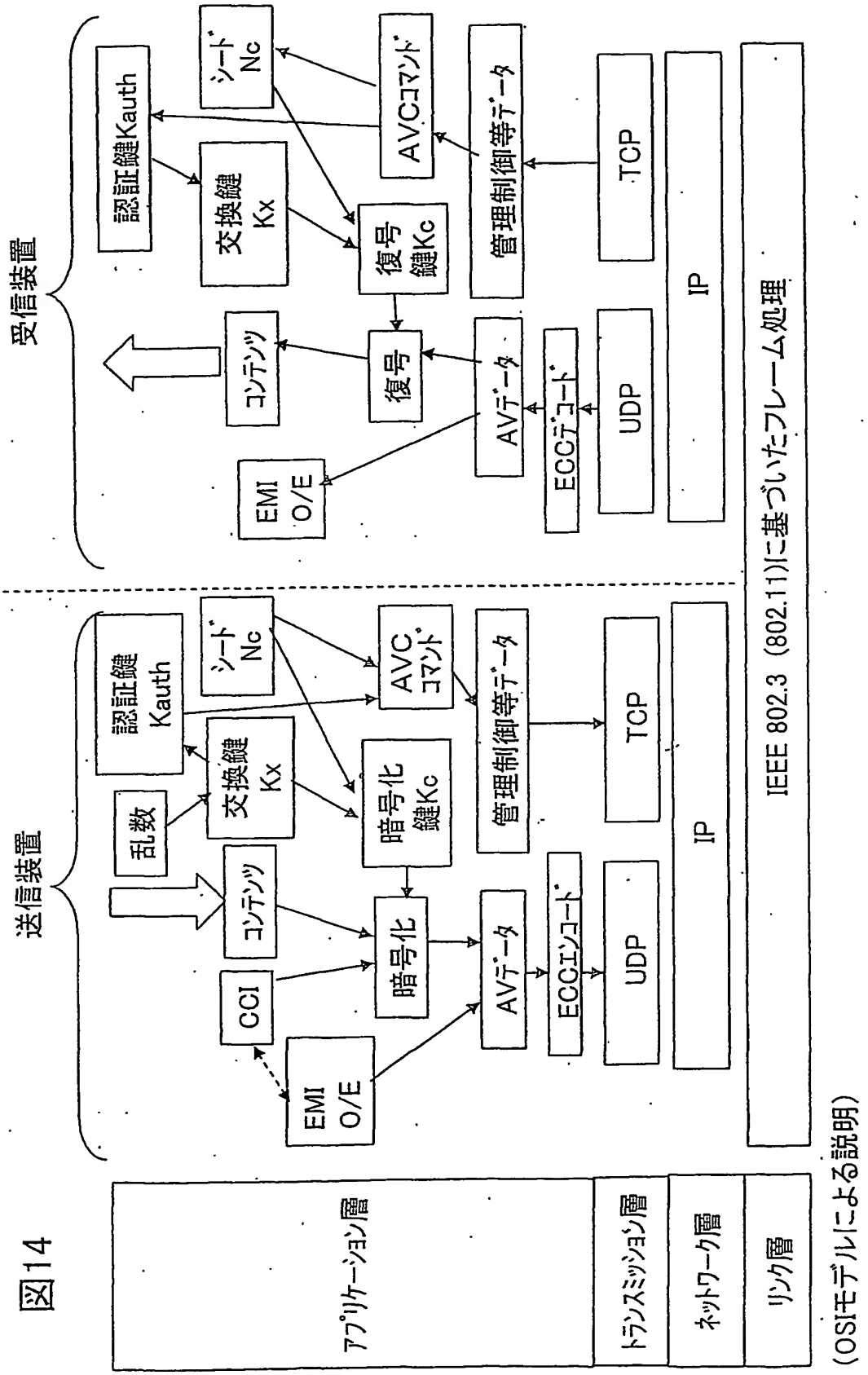

701 第1のパケット化手段
702 第2のパケット化手段
703 第1のパケット受信手段
704 第2のパケット受信手段
403 パケット化手段
405 パケット受信手段
RTP送信処理手段
RTCP/RTSP送信処理手段
UDP処理手段(ポート毎分類)
TCP/UDP処理手段(ポート毎分類)
IP層処理手段(IPヘッダー付加)
RTP受信処理手段
RTCP/RTSP受信処理手段
UDP処理手段(フィルタリング)
TCP/UDP処理手段(フィルタリング)
IP層処理手段(フィルタリング)

図12

図13

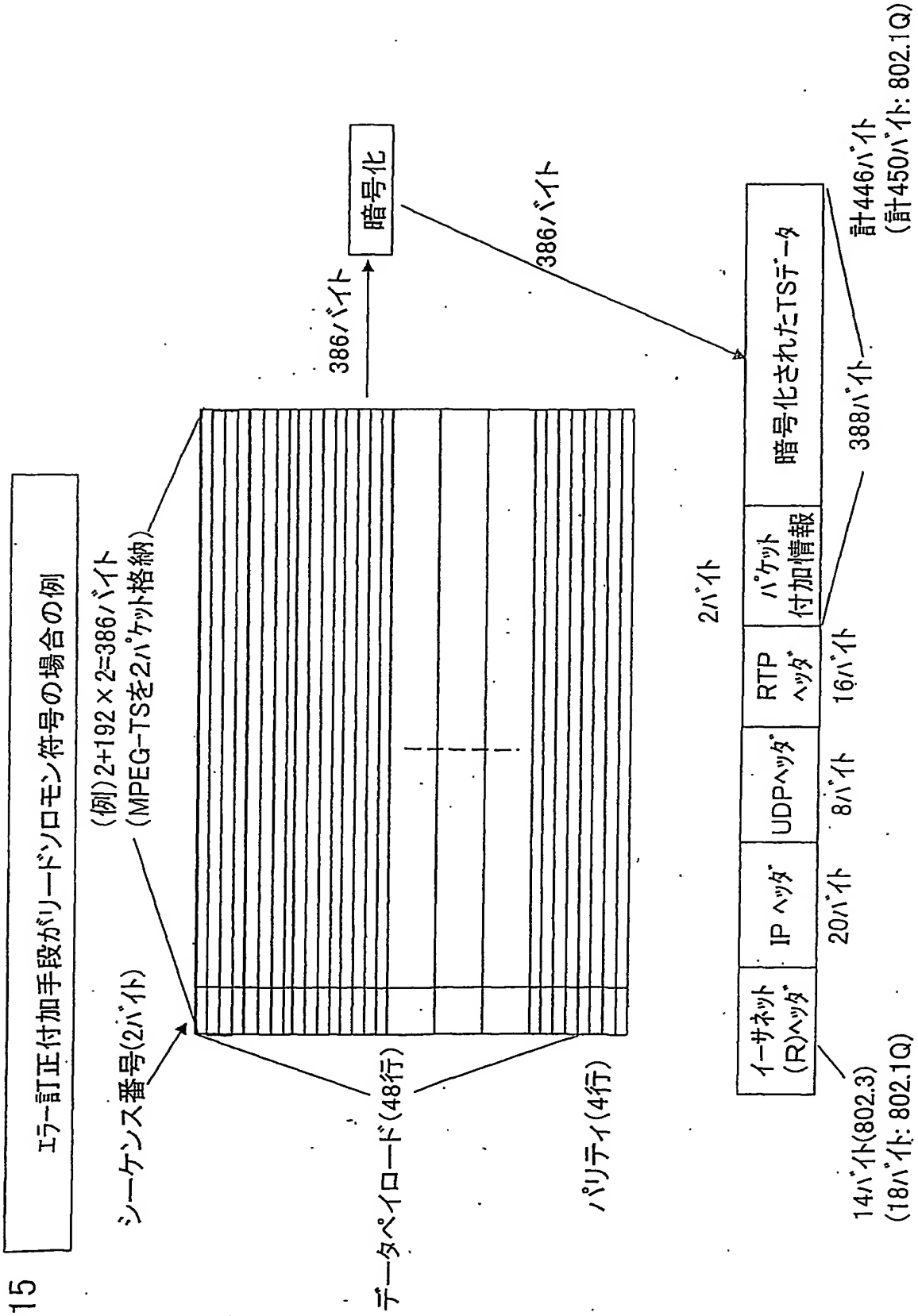
403A パケット化手段
405A パケット受信手段
701 第1の パケット化手段
702A 第2の パケット化手段
703 第1のパケット 受信手段
704A 第2のパケット 受信手段
エラー訂正符号 付加手段
RTP 送信処理手段
RTCP/RTSP 送信処理手段
UDP 処理手段 (ポート番号分類)
TCP/UDP 処理手段 (ポート番号分類)
IP層処理手段 (IPヘッダ付加)
エラー訂正符号 復号手段
RTP 受信処理手段
RTCP/RTSP 受信処理手段
UDP 処理手段 (フィルタリング)
TCP/UDP 処理手段 (フィルタリング)
IP層処理手段 (フィルタリング)

図14



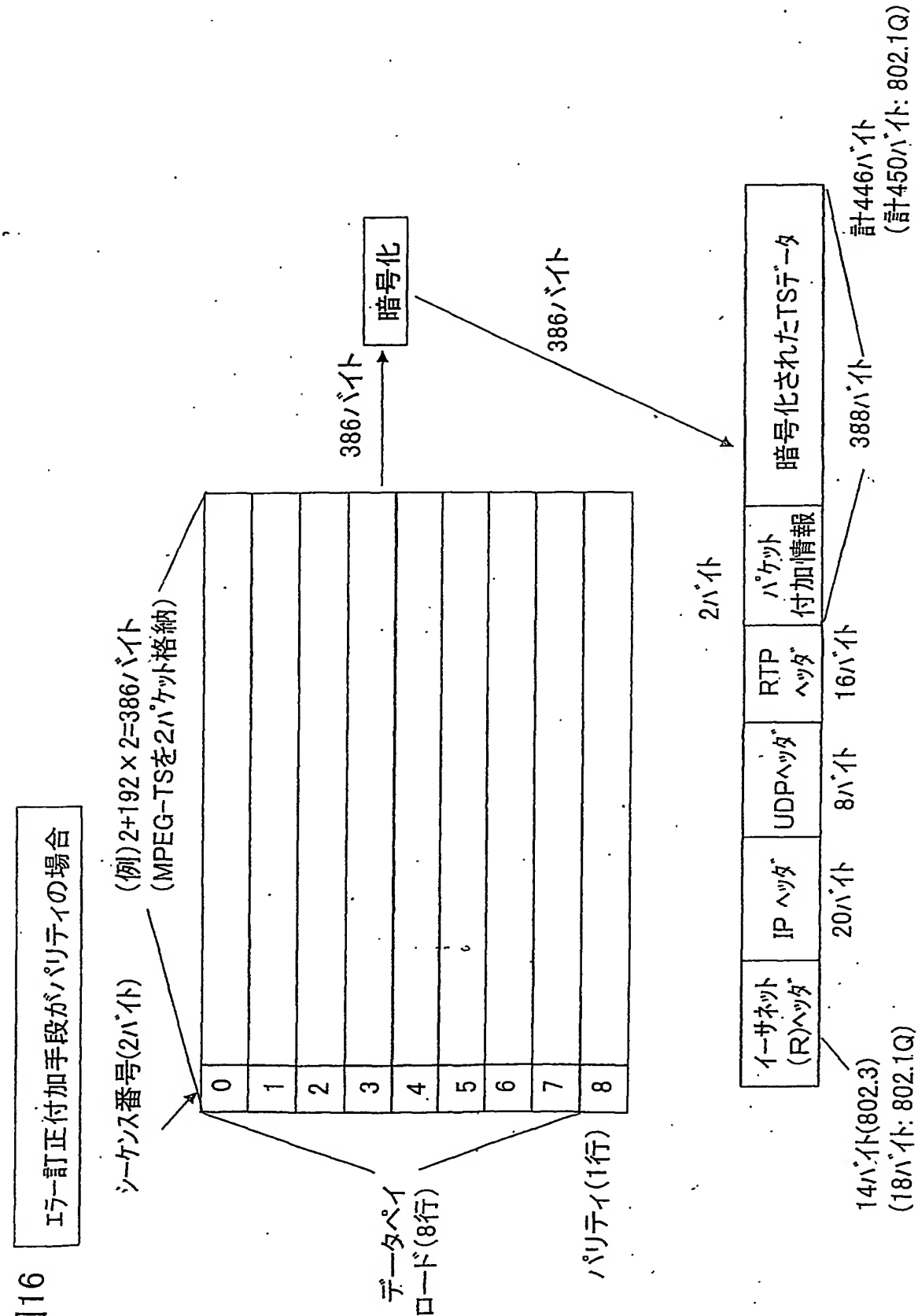
差替え用紙（規則26）

図15



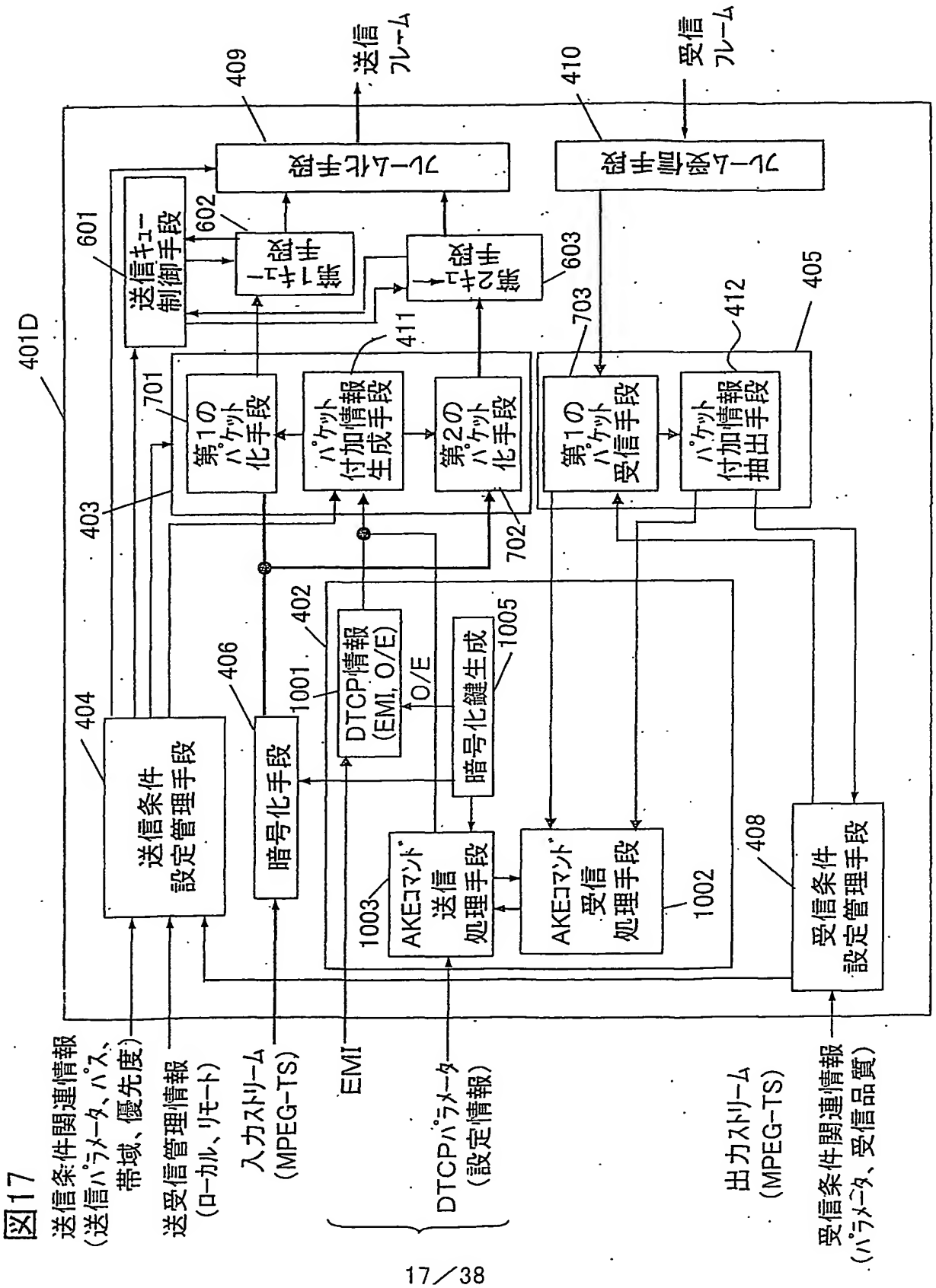
差替え用紙（規則26）

図16



差替え用紙（規則26）

図17



差替え用紙（規則26）

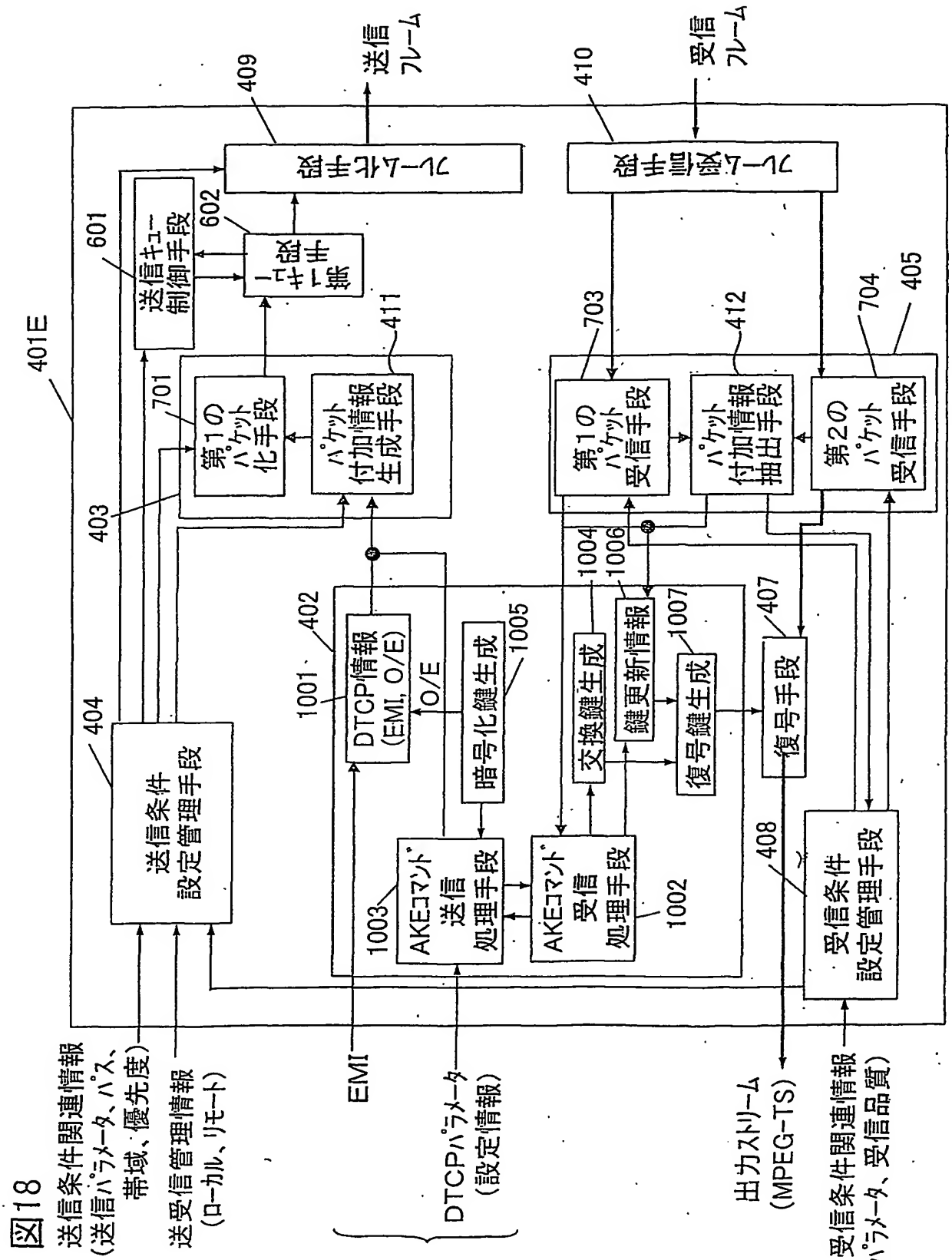
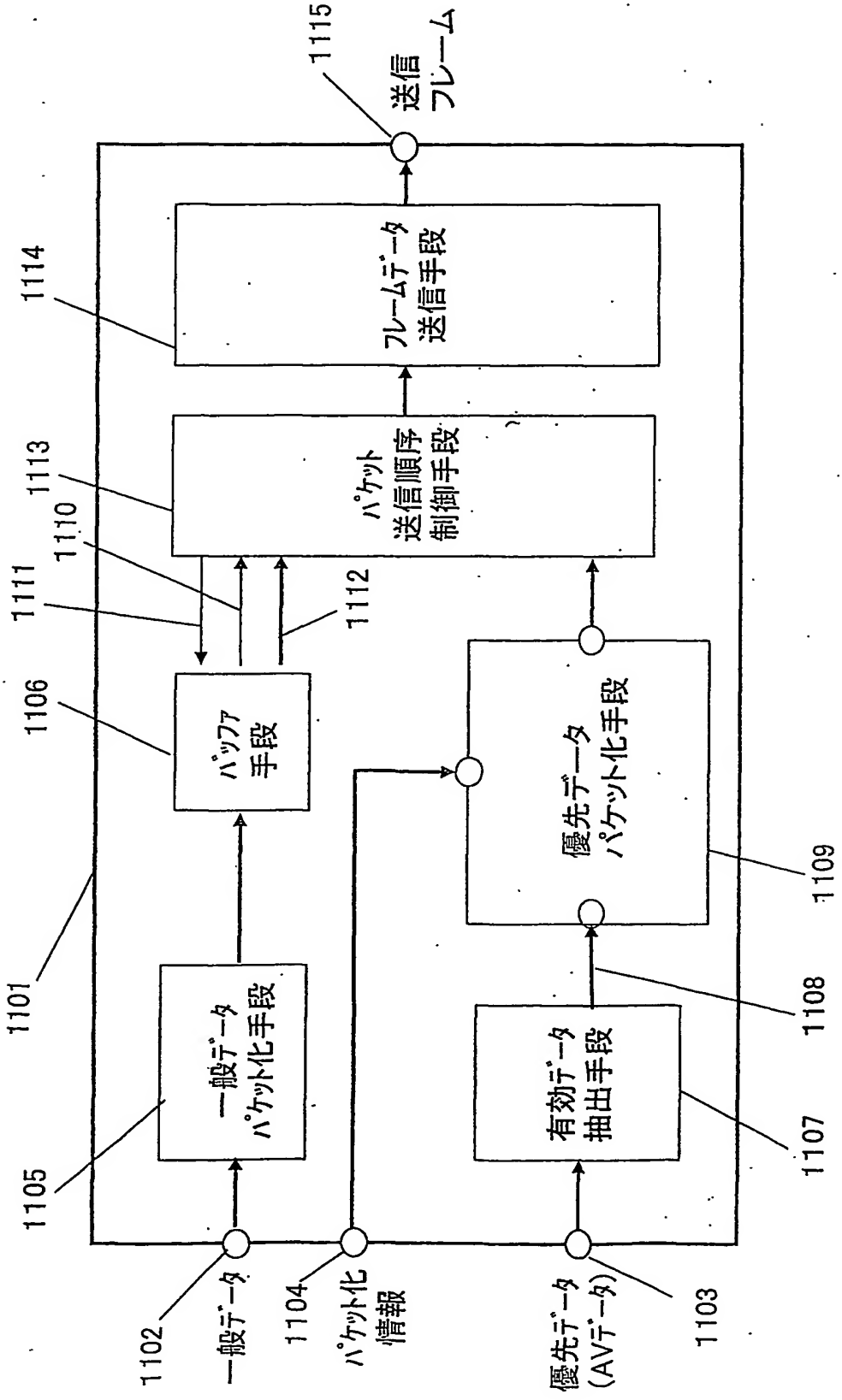


図18

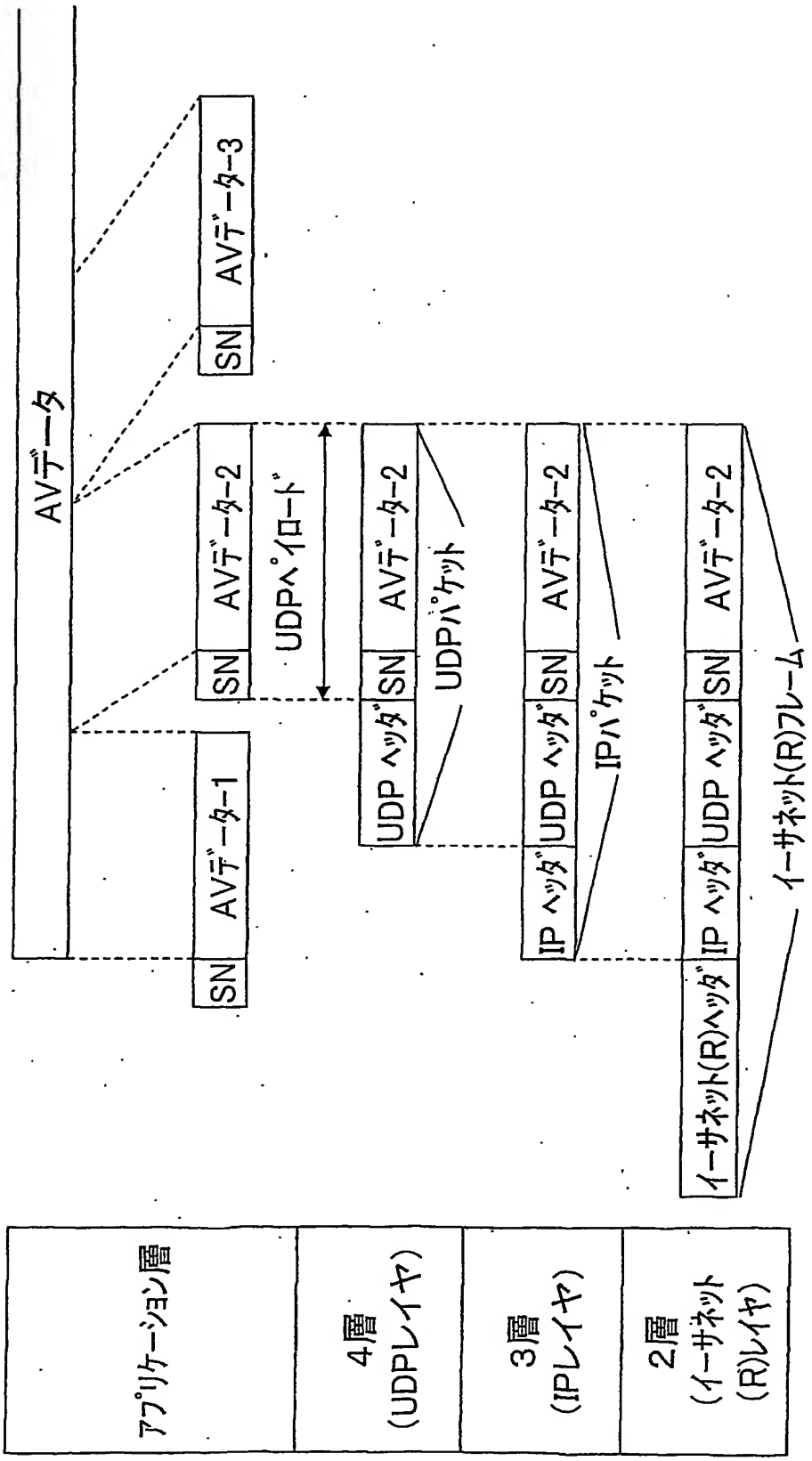
差替え用紙（規則26）

図19



差替え用紙（規則26）

図20



(OSIモデルによる表現)

差替え用紙（規則26）

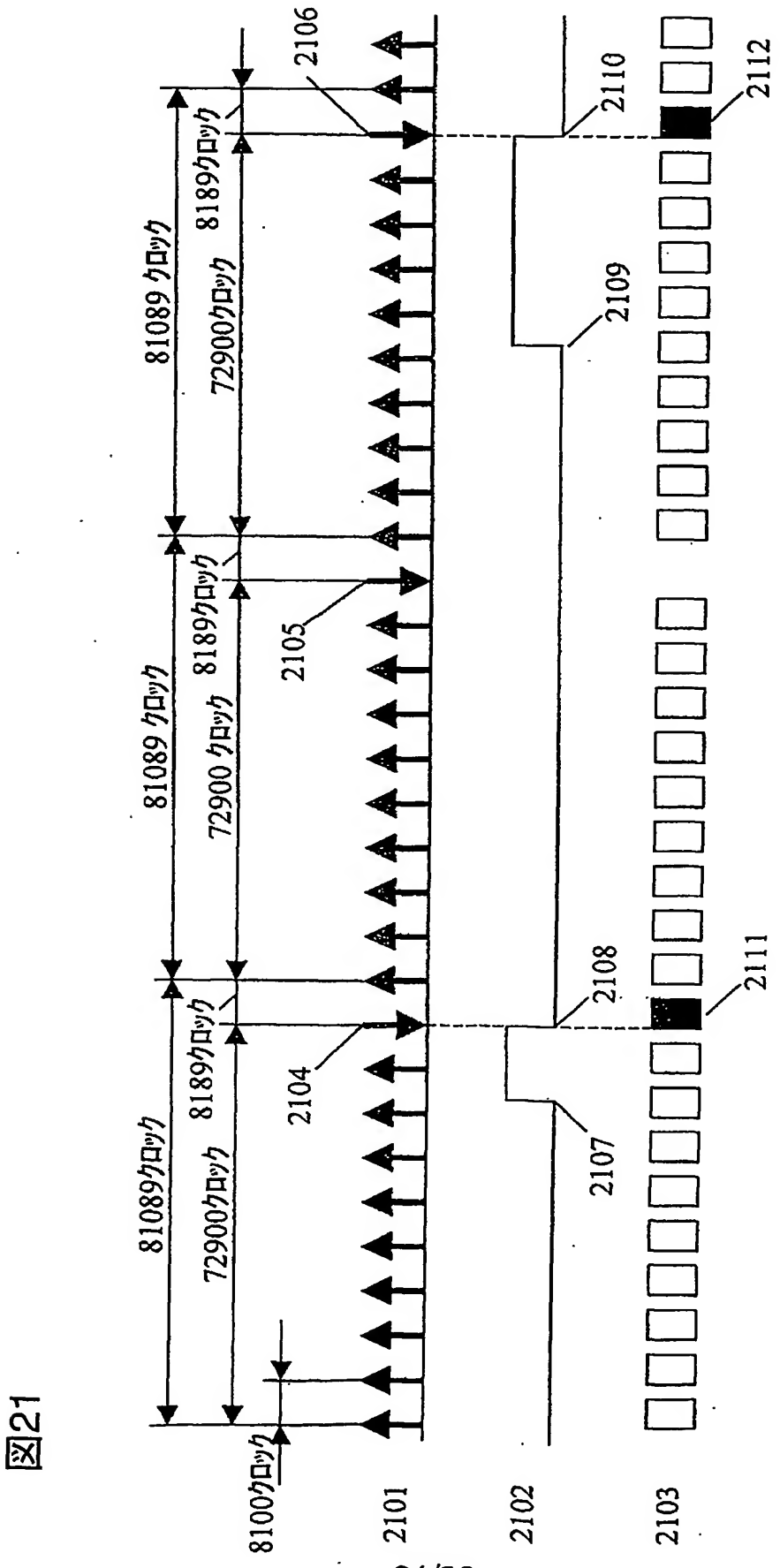

81089ヵロッヵ
8189ヵロッヵ
72900ヵロッヵ
81089ヵロッヵ
8189ヵロッヵ
72900ヵロッヵ
81089ヵロッヵ
8189ヵロッヵ
72900ヵロッヵ
8100ヵロッヵ
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112

図21

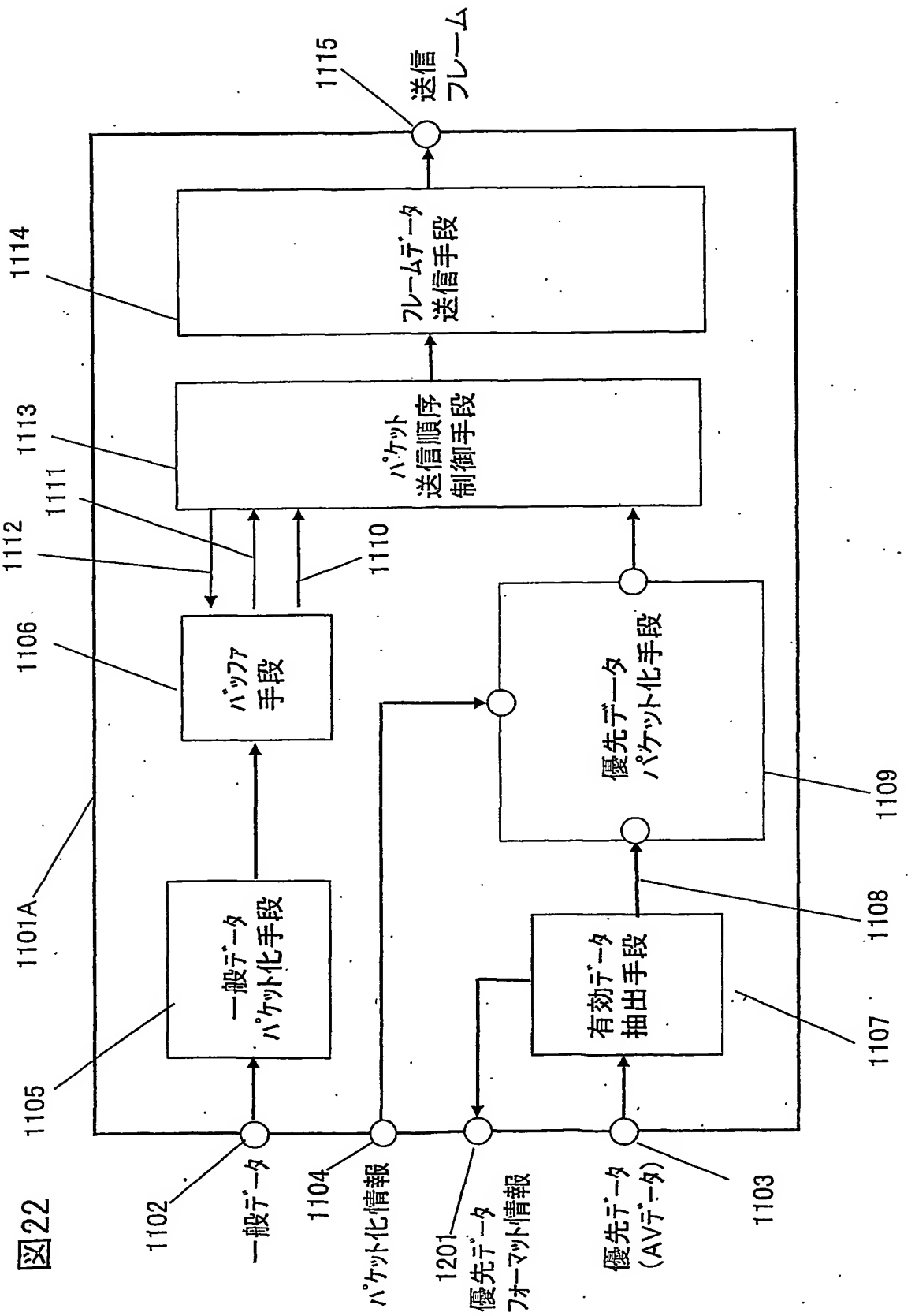


図22

差替え用紙（規則26）

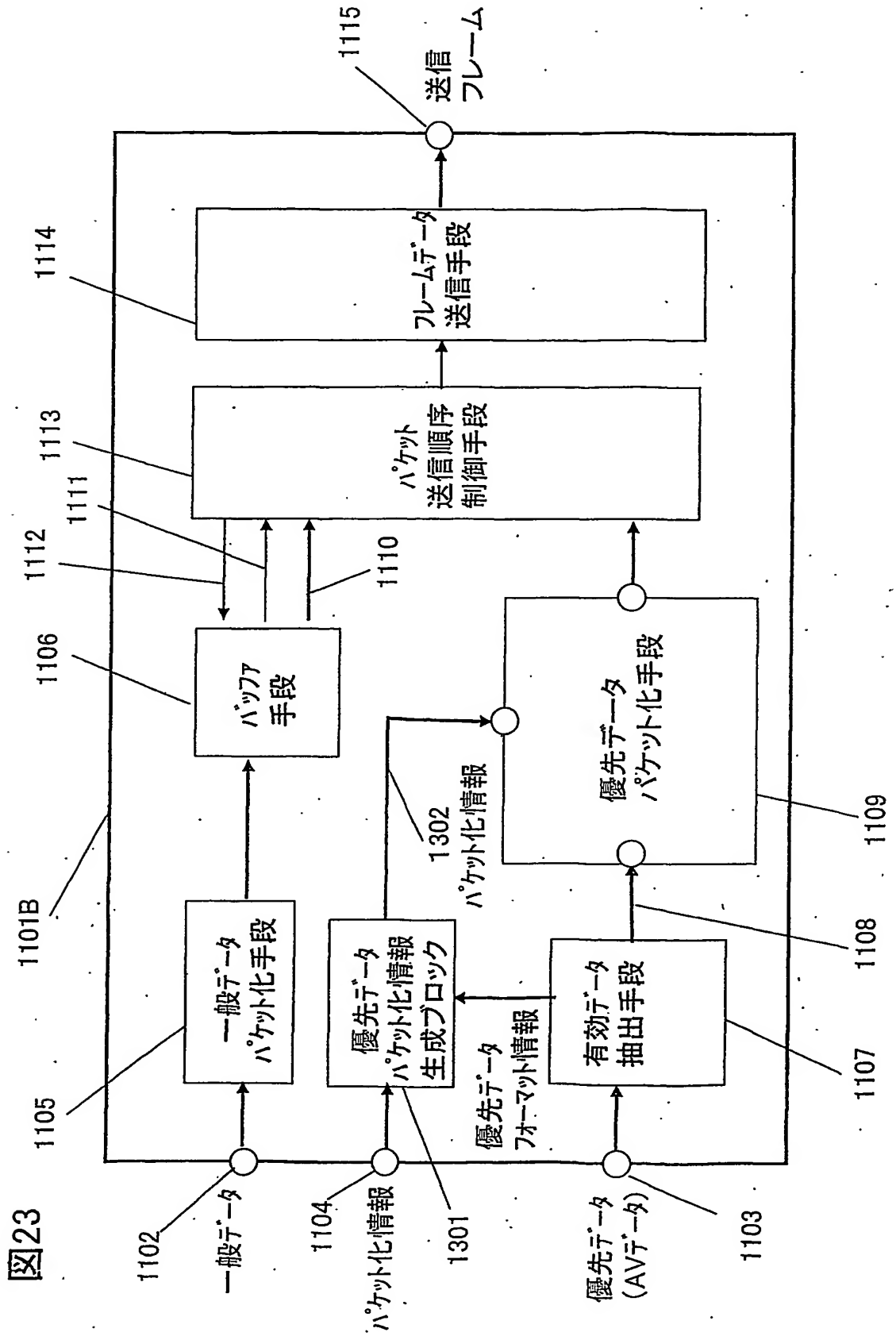


図23

差替え用紙（規則26）

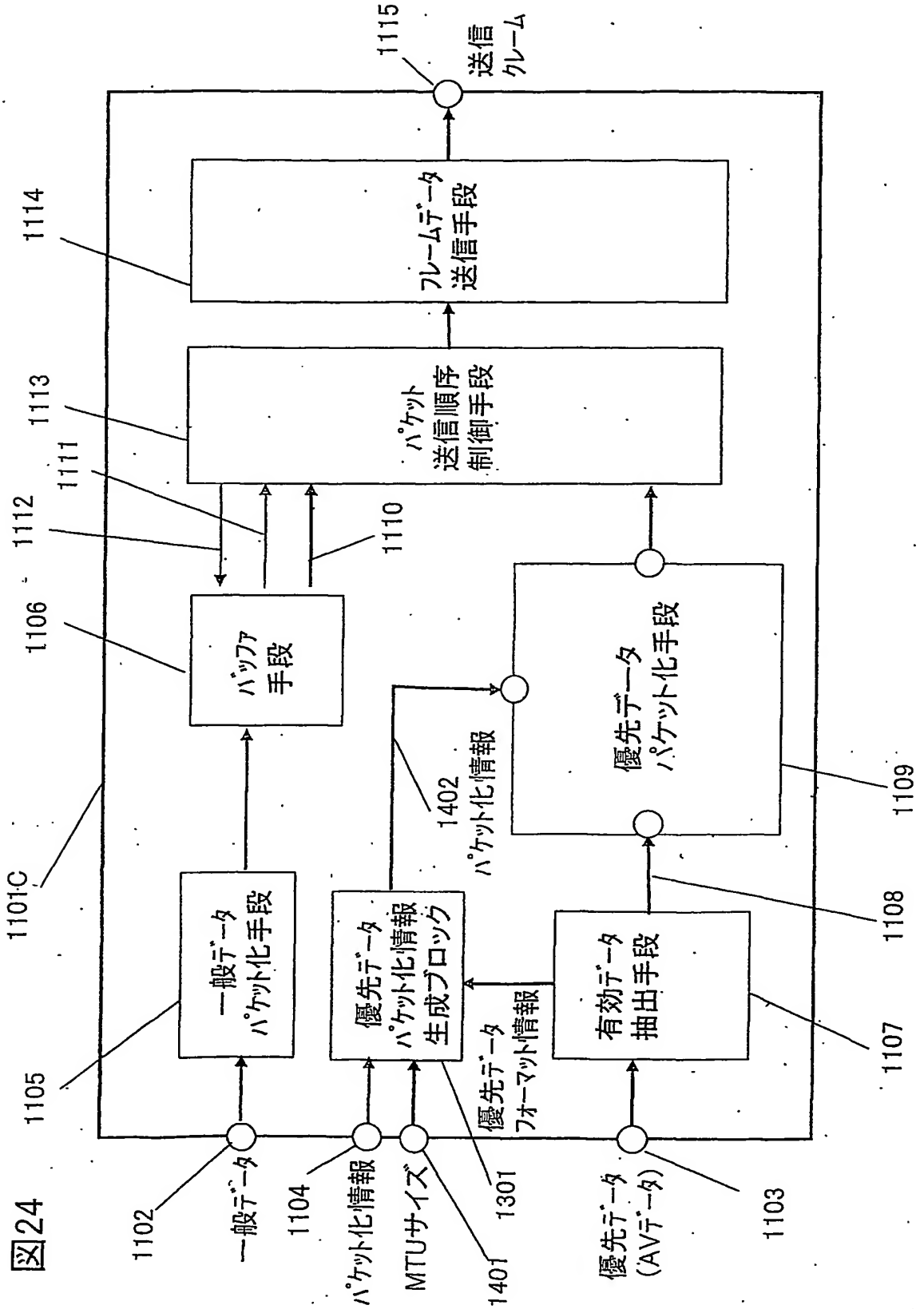
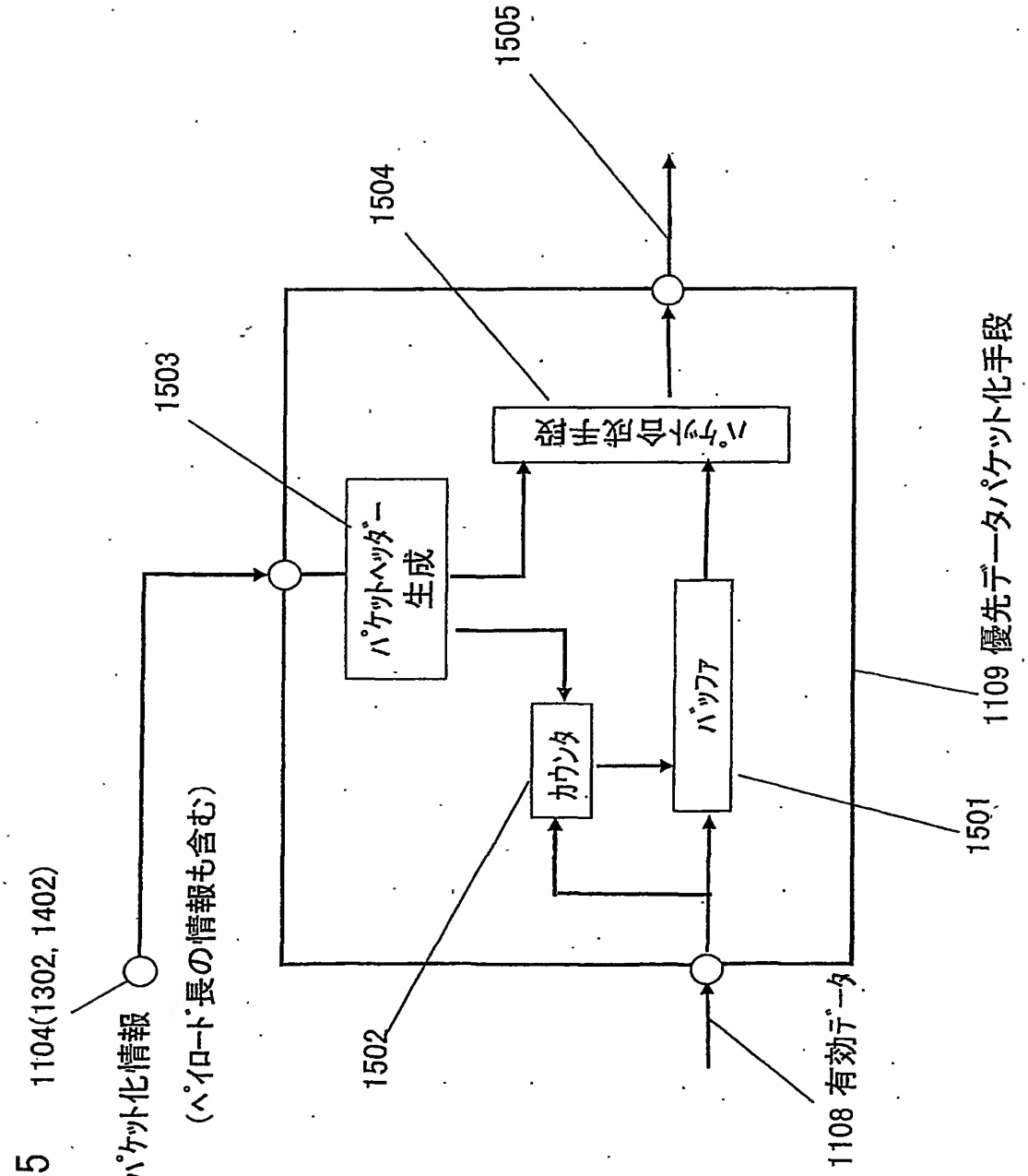


図24

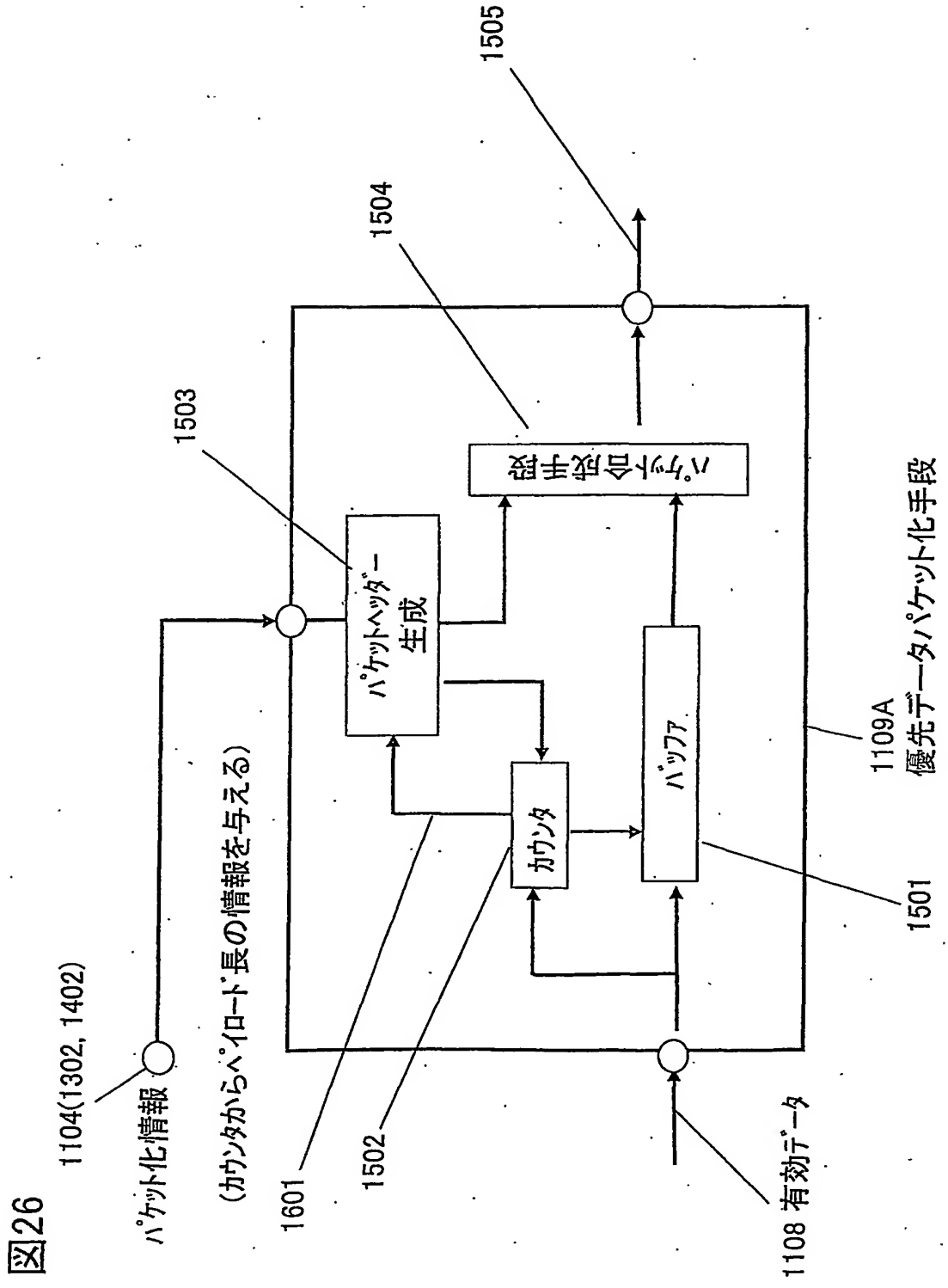
差替え用紙（規則26）

図25



差替え用紙（規則26）

図26



差替え用紙（規則26）

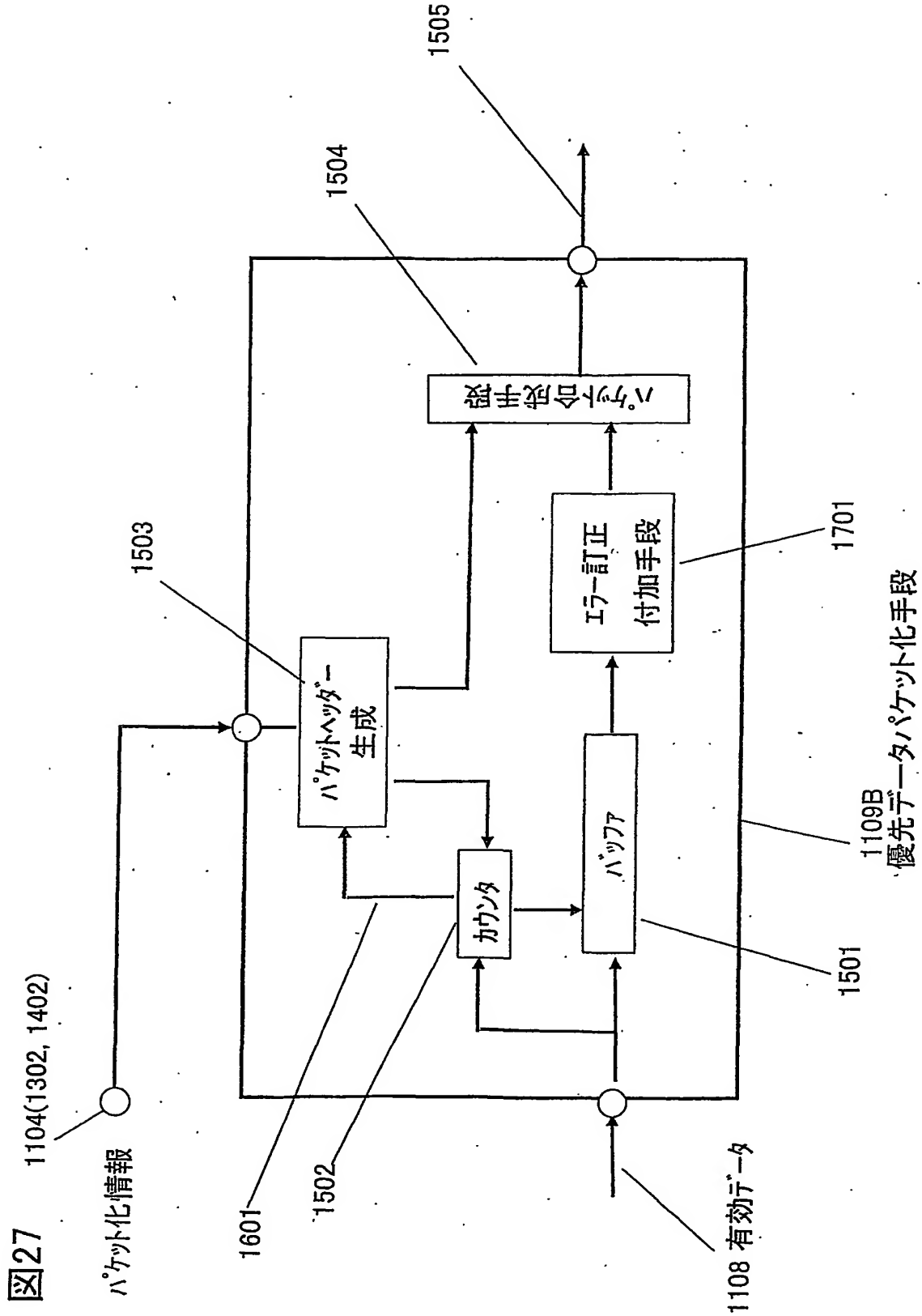

1505
1504
パケット合成手段
1503
パケットヘッダー生成
エラー訂正付加手段
1701
1109B
優先データパケット化手段
バッファ
カウンタ
1501
1601
1502
1104(1302, 1402)
パケット化情報
1108 有効データ

図27

図28

エラー訂正付加手段がリードソロモン符号の場合

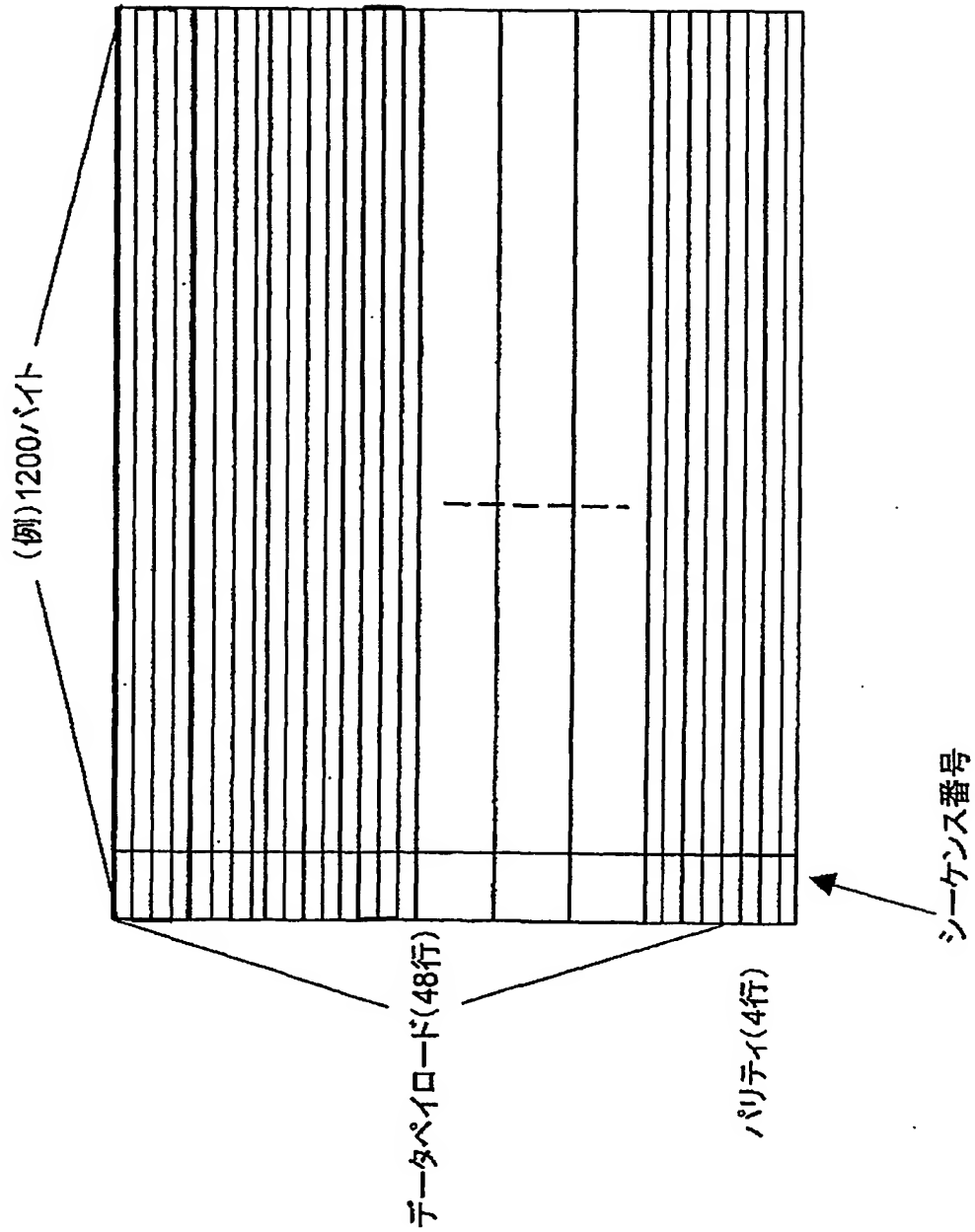
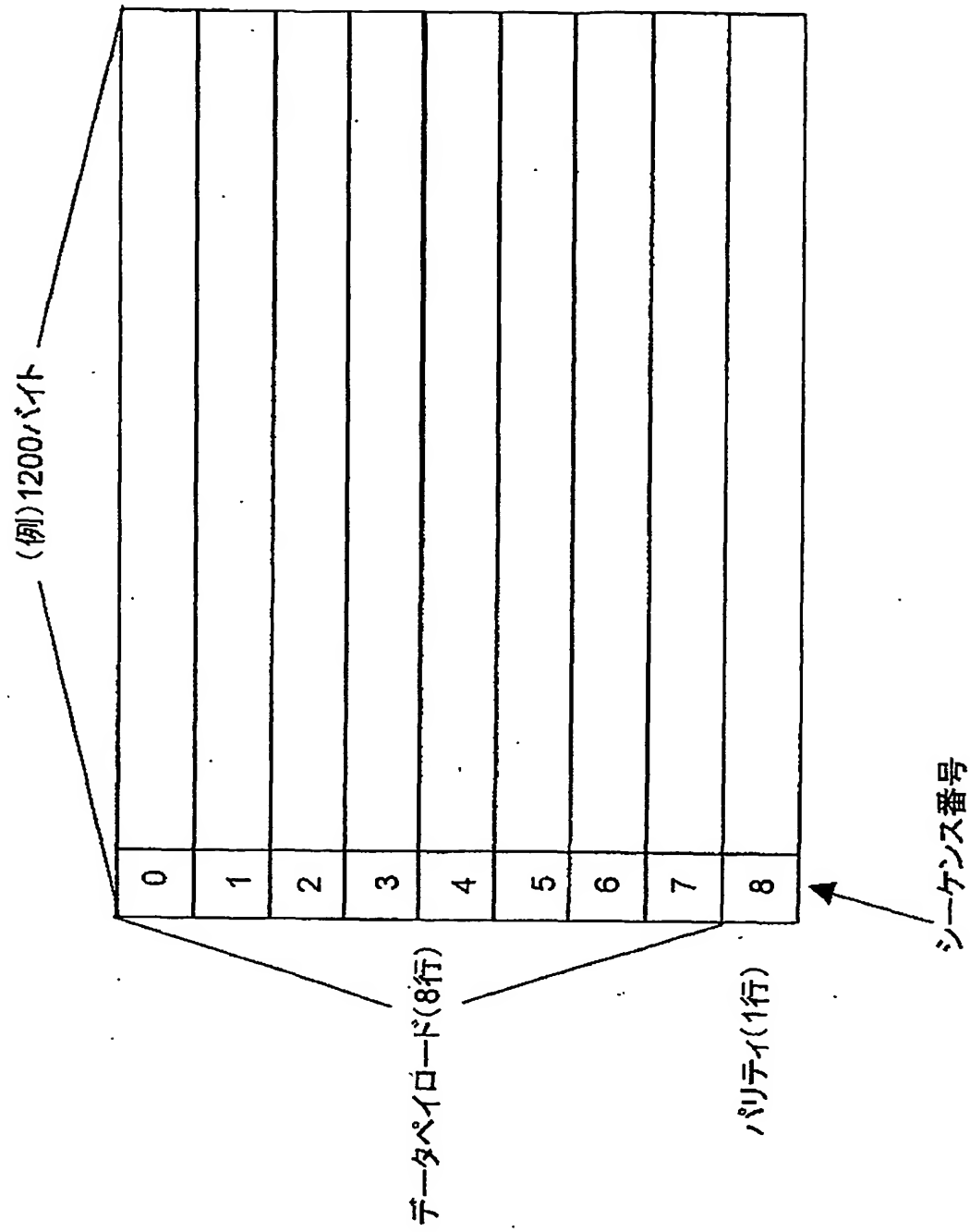


図29

エラー訂正付加手段がパリティの場合



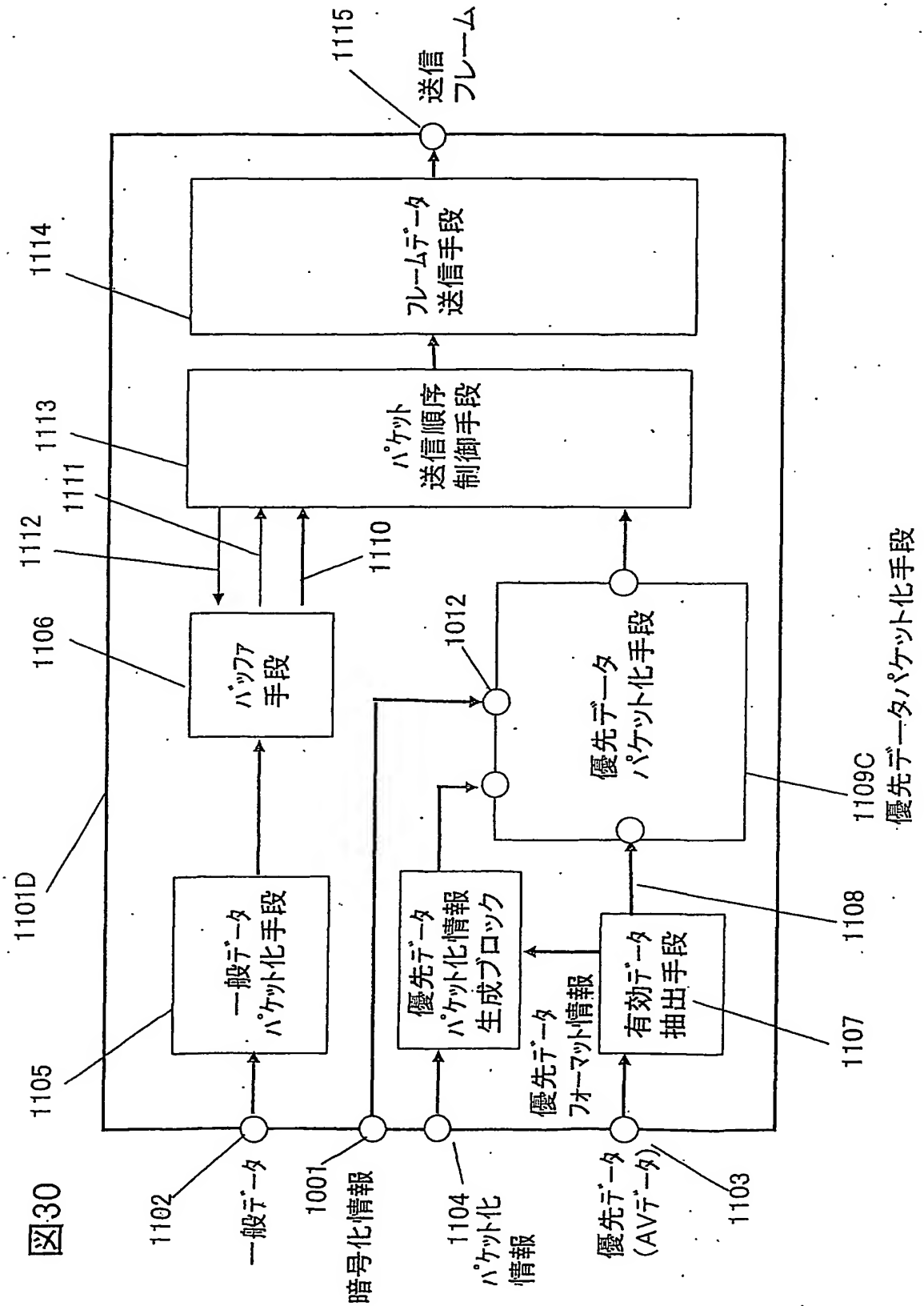
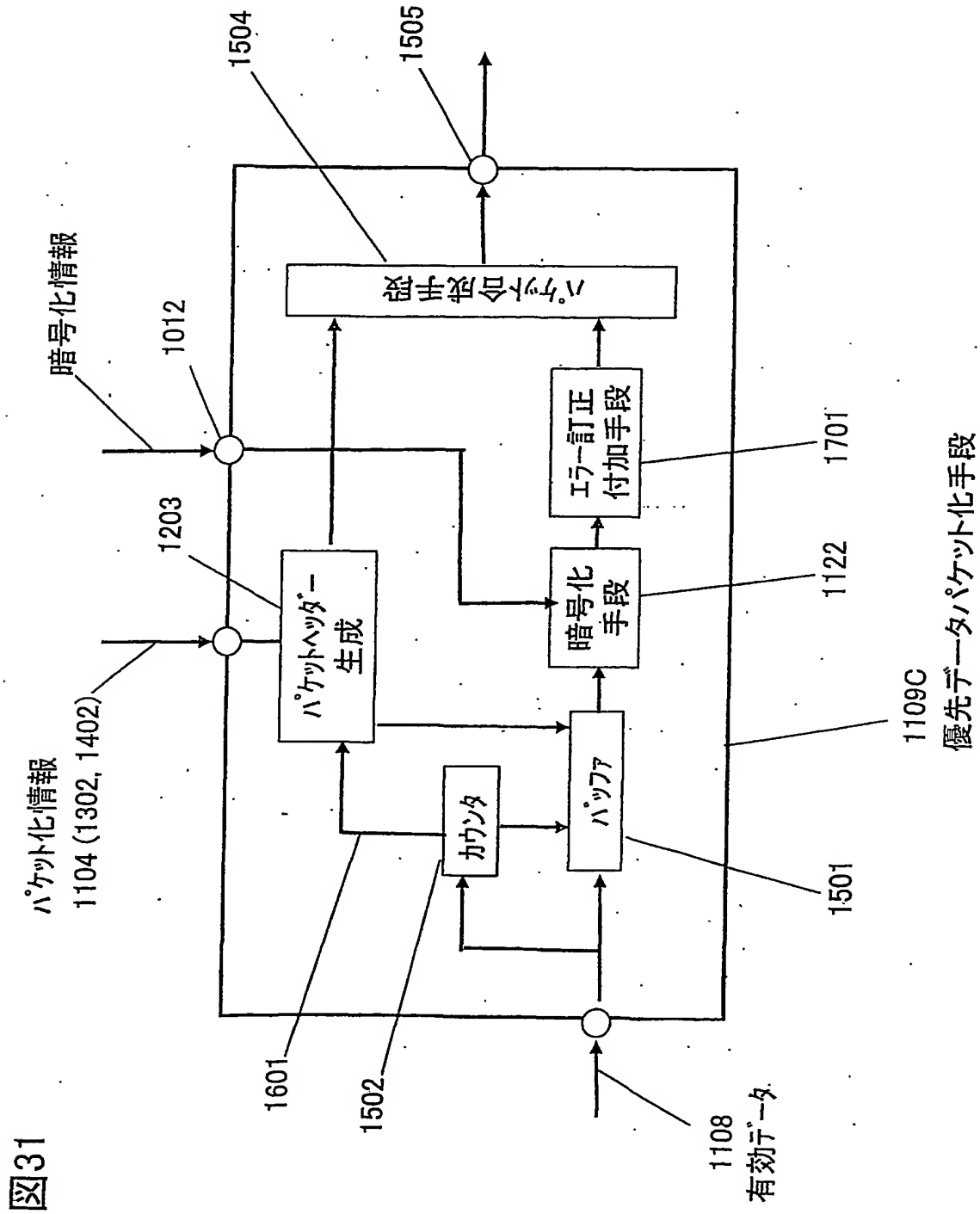


図30

差替え用紙（規則26）

図31



差替え用紙（規則26）

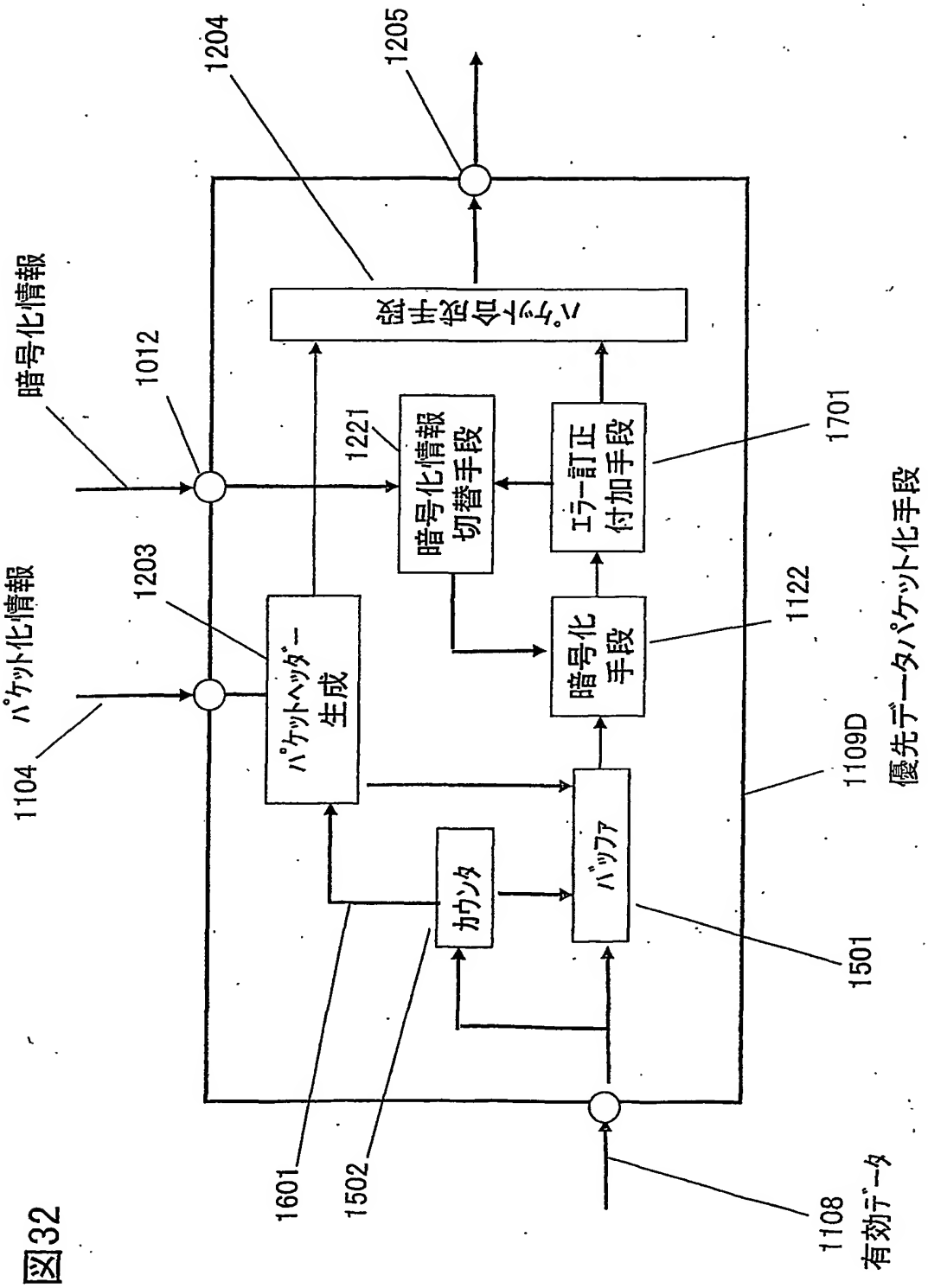
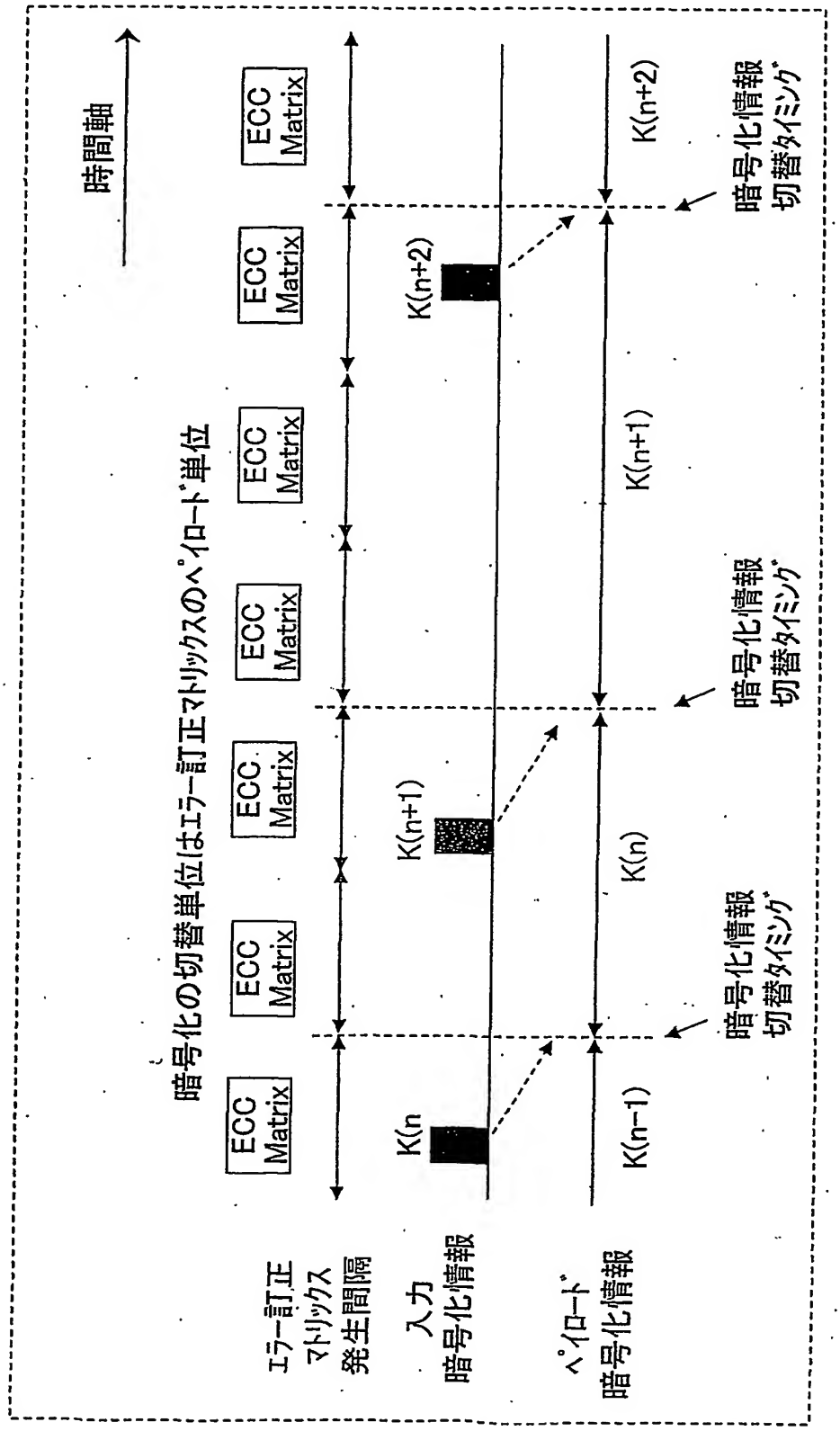

1204
1205
パケット合成手段
暗号化情報
1012
1221
暗号化情報切替手段
エラー訂正付加手段
1701
パケット化情報
1203
パケットヘッダー生成
暗号化手段
1122
1104
1109D
優先データパケット化手段
カウンタ
バッファ
1501
1601
1502
1108
有効データ

図32

図33



差替え用紙（規則26）

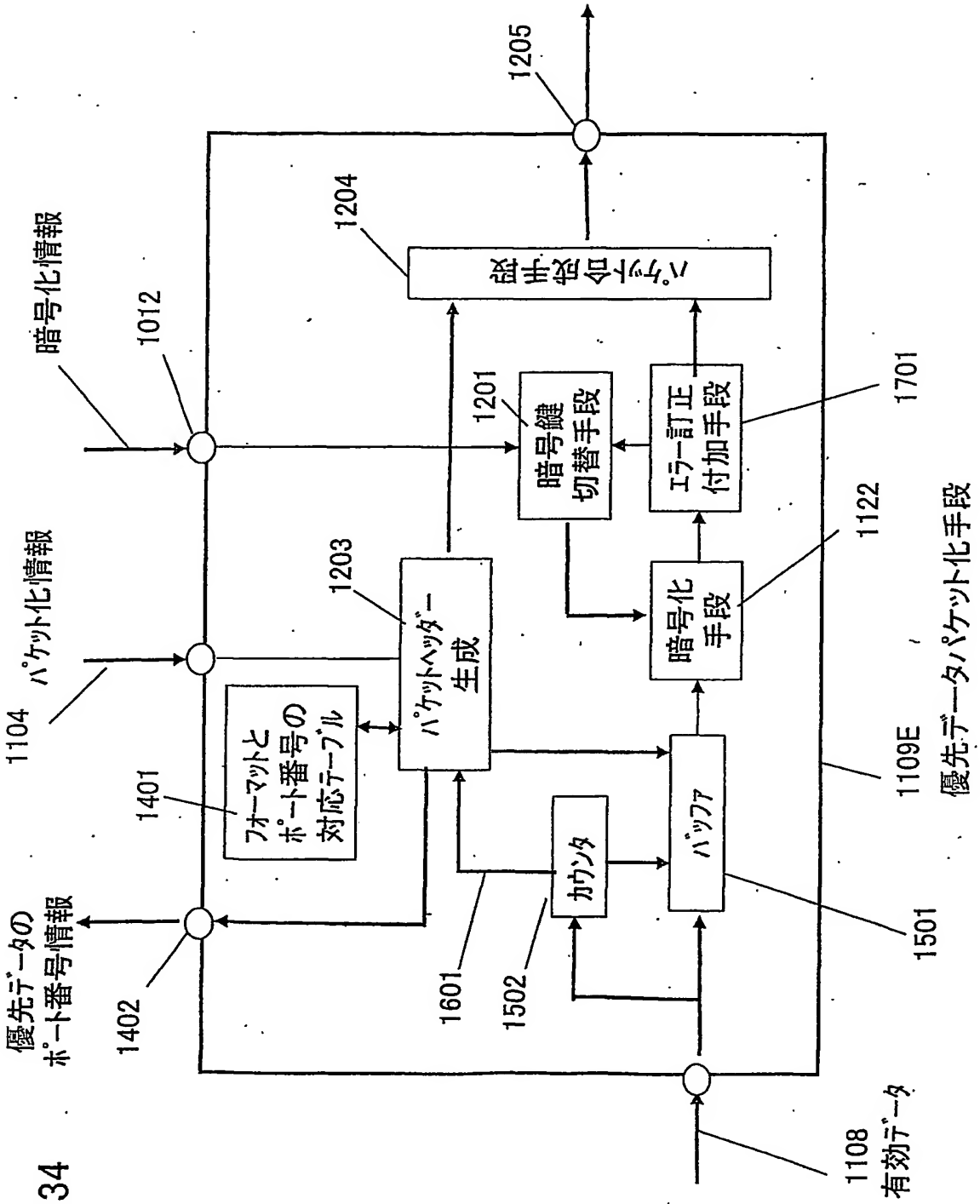

1205
1204
パケット送出部
暗号化情報
1012
1201
暗号鍵
切替手段
エラー訂正
付加手段
1701
パケット化情報
1104
1203
パケットヘッダー
生成
暗号化
手段
1122
フォーマットと
ポート番号の
対応テーブル
1401
カウンタ
バッファ
1109E
優先データパケット化手段
優先データの
ポート番号情報
1402
1601
1502
1501
1108
有効データ

図34

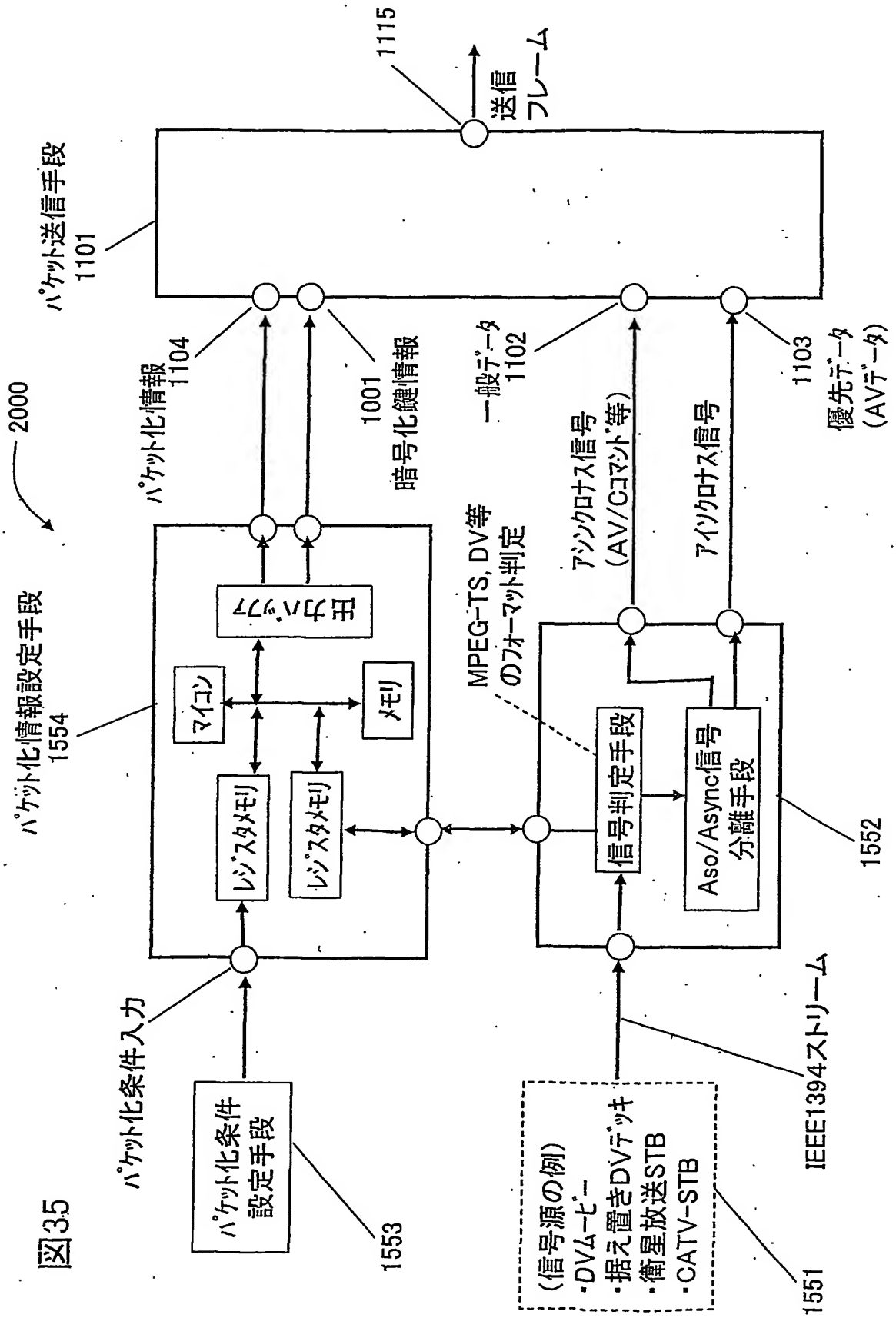


図35

差替え用紙（規則26）

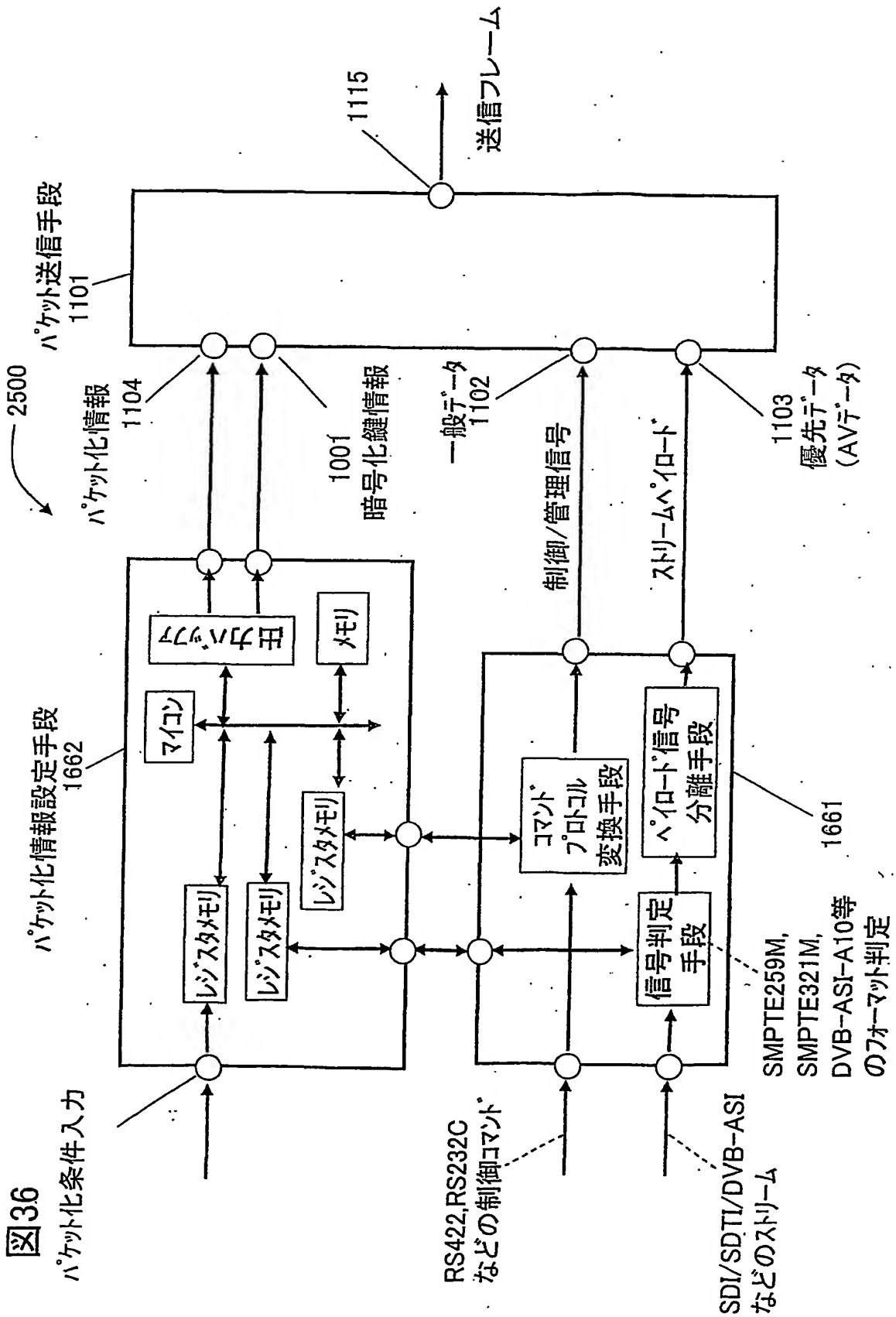


図36

差替え用紙（規則26）

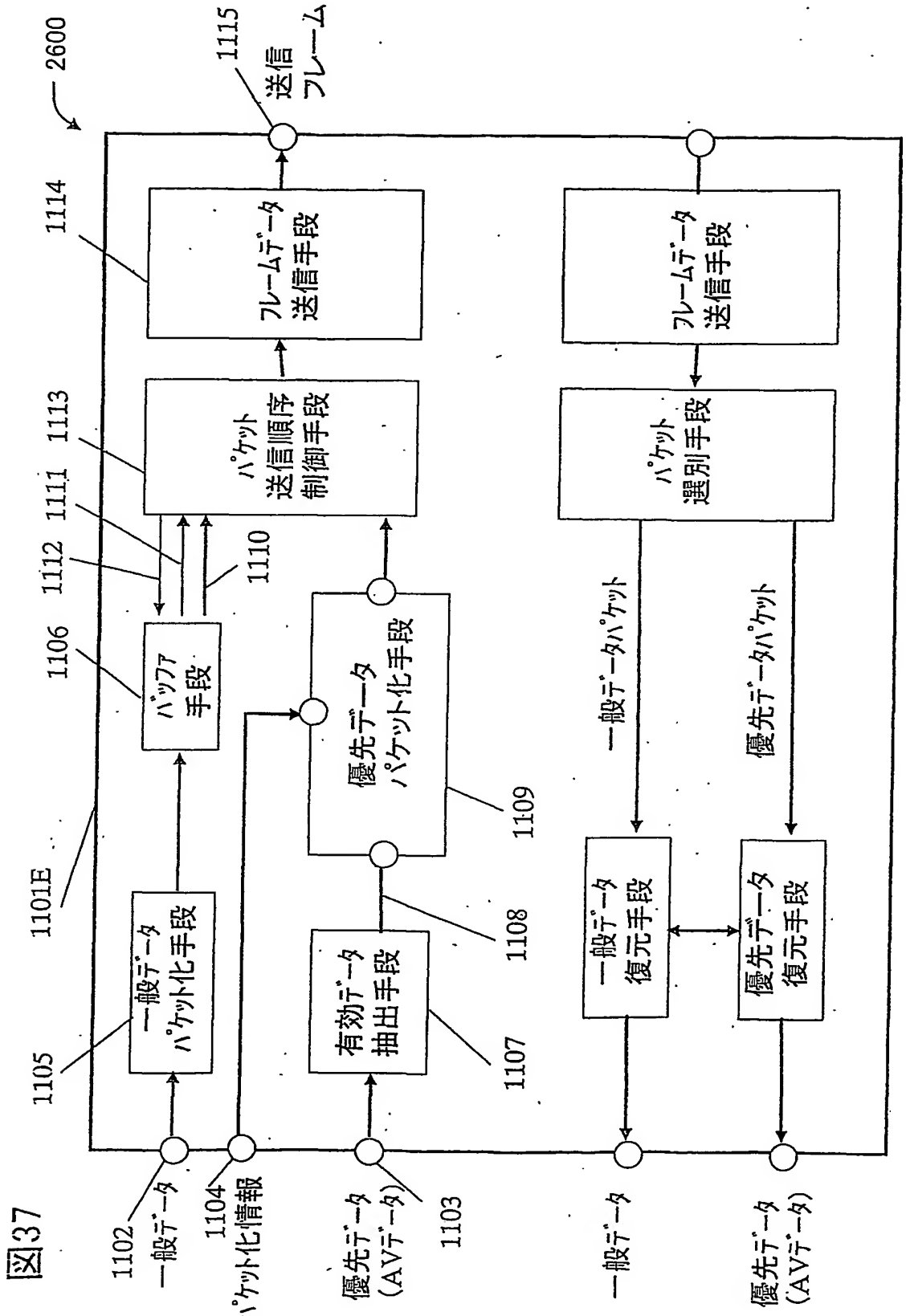


図37

差替え用紙（規則26）

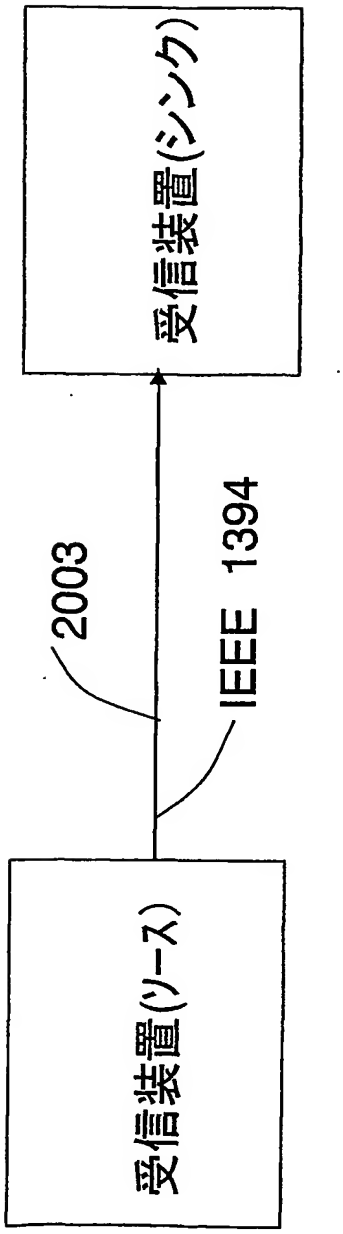


図38

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/13218

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/56, H04L9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/56, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 2002-202720 A (Toshiba Corp.), 19 July, 2002 (19.07.02), Abstract & EP 1220079 A2 & US 2003/0126458 A1	1-3,11-13 4-7,9,10, 14-24,26-28, 31-33,40-46 8,25,29,30, 34-39,47-51
X Y A	JP 2000-341324 A (NTT Data Corp.), 08 December, 2000 (08.12.00), Par. No. [0002] (Family: none)	1-3,11-13 4-7,9,10, 14-24,26-28, 31-33,40-46 8,25,29,30, 34-39,47-51

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 04 December, 2003 (04.12.03)	Date of mailing of the international search report 16 December, 2003 (16.12.03)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/13218

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2000-299686 A (NEC Corp.), 24 October, 2000 (24.10.00), Abstract (Family: none)	4-7,9,16-24, 40-45 8
Y	JP 2002-217961 A (Fujitsu Ltd.), 02 August, 2002 (02.08.02), Claim 2 & US 2002/0097733 A1	9
Y	Michiya TAKADA, Yoshihisa MIWA, "Tokushu 2 Internet no Kiban 'IP o Shiru'", Nikkei Network, Nikkei Business Publications, Inc., No.30, 22 September, 2002 (22.09.02), pages 124 to 139; "Yakuwari 3 Packet o Bunkatsu Suru Toru Kaisen ni Awasete Okisa o Chosei" (pages 132 to 135)	10,42-45
Y	JP 2001-186173 A (Matsushita Electric Industrial Co., Ltd.), 06 July, 2001 (06.07.01), Par. No. [0153] & US 6636481 B1 & CN 1264233 A	14,15
Y	Michiya TAKADA, "Internet ni yoru Anzen na LAN-kan Tsushin VPN o Oku made Saguru", Nikkei Network, Nikkei Business Publications, Inc., No.25, 22 April, 2002 (22.04.02), pages 51 to 69; Figs. 2 to 4 (page 65)	16-24,40-45
Y	JP 2002-26906 A (Mitsubishi Electric Corp.), 25 January, 2002 (25.01.02), Par. No. [0037] (Family: none)	18-21,40-45
Y	JP 2002-232955 A (Denso Corp.), 16 August, 2002 (16.08.02), Claims 1 to 3 (Family: none)	26-28,31,32
Y A	JP 11-196081 A (Kabushiki Kaisha Kodo Ido Tsushin Security Gijutsu Kenkyusho), 21 July, 1999 (21.07.99), Par. No. [0003] (Family: none)	33,46 34-39,47-51
Y	JP 7-297831 A (Sumitomo Electric Industries, Ltd.), 10 November, 1995 (10.11.95), Par. No. [0038] (Family: none)	41

国際調[redacted]告　　国際出願番[redacted]PCT／JP03／13218

A.　発明の属する分野の分類（国際特許分類（IPC））
Int. Cl⁷ H04L12／56, H04L 9／00

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int. Cl⁷ H04L12／56, H04L 9／00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1926－1996年
日本国公開実用新案公報　1971－2003年
日本国登録実用新案公報　1994－2003年
日本国実用新案登録公報　1996－2003年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	JP　2002－202720　A（株式会社東芝） 2002．07．19 要約 &EP　1220079　A2	1-3, 11-13 4-7, 9, 10, 14-24, 26-28, 31-33, 40-46
A	&US　2003／0126458　A1	8, 25, 29, 30, 34-39, 47-51

[x] C欄の続きにも文献が列挙されている。　[ ] パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
04．12．03	16.12.03

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5X	3047
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目４番３号	石井　研一 印		
	電話番号　03－3581－1101　内線　3596		

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告 | 国際出願番号 PCT／JP03／13218

C（続き）． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y A	ＪＰ ２０００－３４１３２４ Ａ（株式会社エヌ・ティ・ティ・データ） ２０００．１２．０８ 第0002段落 （ファミリーなし）	1-3, 11-13 4-7, 9, 10, 14-24, 26-28, 31-33, 40-46 8, 25, 29, 30, 34-39, 47-51
Y A	ＪＰ ２０００－２９９６８６ Ａ（日本電気株式会社） ２０００．１０．２４ 要約 （ファミリーなし）	4-7, 9, 16-24, 40-45, 8
Y	ＪＰ ２００２－２１７９６１ Ａ（富士通株式会社） ２００２．０８．０２ 請求項２ ＆ＵＳ ２００２／００９７７３３ Ａ１	9
Y	高田 学也，三輪 芳久，“特集２ インターネットの基盤 「ＩＰを知る」”，日経ネットワーク，日経ＢＰ社，第30号， ２００２．０９．２２，pp. 124-139 “役割３ パケットを分割する 通る回線に合わせて大きさを調整”（pp. 132-135）	10, 42-45
Y	ＪＰ ２００１－１８６１７３ Ａ（松下電器産業株式会社） ２００１．０７．０６ 第0153段落 ＆ＵＳ ６６３６４８１ Ｂ１ ＆ＣＮ １２６４２３３ Ａ	14, 15
Y	高田 学也，“インターネットによる安全なＬＡＮ間通信 ＶＰＮを奥まで探る”，日経ネットワーク，日経ＢＰ社，第25号， ２００２．０４．２２，pp. 51-69 第2-4図（p. 65）	16-24, 40-45
Y	ＪＰ ２００２－２６９０６ Ａ（三菱電機株式会社） ２００２．０１．２５ 第0037段落 （ファミリーなし）	18-21, 40-45
Y	ＪＰ ２００２－２３２９５５ Ａ（株式会社デンソー） ２００２．０８．１６ 請求項１－３ （ファミリーなし）	26-28, 31, 32

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y A	ＪＰ　１１－１９６０８１　Ａ（株式会社高度移動通信セキュリティ技術研究所）　１９９９．０７．２１ 第0003段落 （ファミリーなし）	33, 46 34-39, 47-51
Y	ＪＰ　７－２９７８３１　Ａ（住友電気工業株式会社） １９９５．１１．１０ 第0038段落 （ファミリーなし）	41